www.monografias.com

# Aproximación a los perfiles de personalidad

# de los sujetos que realizaron delitos informáticos

**Tesis de licenciatura**

1. [**Resumen**](#resum)
2. [**Composición del mundo actual**](#composic)
3. [**Las redes: la red Internet**](#redes)
4. [**Los delitos informáticos**](#delitos)
5. [**Estudios psicológicos de los delincuentes informáticos**](#estudios)
6. [**Materiales, métodos y procedimientos**](#material)
7. [**Presentación y análisis de resultados**](#analisis)
8. [**Conclusiones**](#concl)
9. [**Anexos**](#anexo)
10. [**Bibliografía**](#biblio)

**Resumen**

Los objetivos de esta investigación fueron conocer las características de los delitos informáticos; investigar el impacto de estas conductas en la vida social y tecnológica de Occidente durante los últimos cuarenta años y presentar una aproximación a los perfiles de personalidad característicos de los sujetos que realizaron delitos informáticos.

Para ello se analizaron un conjunto de casos individuales sobre delitos informáticos provenientes del exterior de una organización mediante el uso de la red Internet.

Los delitos informáticos son conductas que comienzan a tener implicancias jurídicas cuando dada la virtualidad propiciada en la red Internet se cometen delitos.

Generalmente responde a conductas que no se realizan en un solo acto, sino en una serie continuada de ellos.

Las figuras delictivas presentan diferentes características, porque cada una tiene un objetivo distinto. Una vez producidos, es posible eliminar toda evidencia de su realización, lo que produce dificultades para el descubrimiento y la prueba; y con frecuencia su ilegalidad no es clara, es más, depende el país donde el delito se emita.

Se identificaron los perfiles psicológicos *hacker, cracker, phreaker y virucker,* los que pueden presentarse juntos en un mismo individuo o separados.

**INTRODUCCIÓN**

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono.

La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

Luego nace Internet como una tecnología que pondría a la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo.

El entramado de redes informáticas, traspasa fronteras territoriales, uniendo a la denominada aldea globalizada, transportándonos a un mundo virtual. Logrando la difusión inmediata de un mundo a otro, de noticias, operaciones comerciales, bancarias, cadenas de información que revolucionan y seguramente continuarán revolucionando al mundo.

Así, en la era de la información, las ideas, datos y archivos en la red de una empresa, es probablemente lo más valioso que posee.

A las reconocidas ventajas, debemos encontrarnos con la naturaleza humana de la cual no debemos olvidarnos, porque detrás de una simple computadora o de grandes sistemas informáticos, redes, opera el hombre.

El comportamiento humano tiende a infringir las normas (fueren sociales o jurídicas); con la particularidad que en esta clase de delitos, el autor no responde a los estereotipos del delincuente.

Considerando además la gran posibilidad de no ser descubiertos o denunciados;  siendo por ello más atrayente infringir las reglas.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Para llegar a la formulación de una hipótesis de trabajo se plantearon los siguientes interrogantes:

¿Qué son los delitos informáticos? Cada delito informático presenta diferentes características y por eso los rasgos de personalidad de los autores deberían ser diferentes en cada tipo de delito, ¿o son parecidos?, ¿Cómo son?

¿Cómo son las personas que los realizan?, ¿Cuáles son sus principales motivaciones?, ¿Cómo son considerados estos delitos por el Derecho en otros países y en Argentina? ¿Cuáles son las penas en el caso de estar tipificados como delitos?

Todo esto interesa a la psicología porque supone una modificación importante del perfil psicológico del agresor.

Así en esta investigación se intenta realizar una aproximación psicológica al estudio del fenómeno de los delitos informáticos y de los sujetos detrás de ellos.

**PARTE I - MARCO TEORICO REFERENCIAL**

**Capítulo I**

**Composición del mundo actual**

**1.1 – La globalización**

Tal como se explica en la introducción cuando se identificó el problema que dio origen a esta investigación, ha sido necesario incluir una definición académica de globalización, porque para abordar la temática se requiere una ubicación contextual en ese sentido. No se puede conocer el mundo virtual de los delitos informáticos sin definir el ámbito donde ellos se producen.

La globalización es un sistema económico de alcance mundial “caracterizado por el predominio del comercio libre, intercambios de bienes y servicios muy intensos entre los países centrales como es el caso de los Estados Unidos, la Unión Europea y Japón, gran dependencia y una libertad plena de los movimientos de capital que, apoyada en los avances de la informática y las comunicaciones, posibilita su influencia financiera en todo el planeta”.[[1]](#footnote-1)

Este proceso, aunque muchos no coincidan con los autores señalados, se inició en 1980 como producto del desborde de los espacios económicos que representan los Estados, por parte del capitalismo, cuya “movilidad absoluta de los fondos ha convertido al mundo en un centro financiero único, con masas enormes de capitales que se desplazan y especulan sin registrar fronteras”, y señalan que “uno de sus rasgos más destacados es el relevante papel que han adquirido las corporaciones multinacionales; éstas son depositarias de los resortes fundamentales para su control, que desde luego incluyen la investigación y la tecnología, que constituyen la base de la estructura de la economía mundial y concentran gran parte del poder real que rige los destinos del planeta”. Como dato accesorio se puede mencionar que “en el mundo existen más de 35.000 empresas multinacionales, con una participación en el comercio mundial total del 70%, y más del 40% de las transacciones internacionales de mercancías y servicios se realiza entre multinacionales o entre las casas matrices de éstas y sus filiales, y controlan el 75% de las inversiones mundiales”.[[2]](#footnote-2) Esta política empresaria implica que el grado de concentración de poder económico cada vez se acentúe más. Debe tenerse presente que “los cien grupos industriales mayores del mundo, sin incluir servicios ni financieros, ocupan más de 14 millones de personas, poseen una gran influencia en las relaciones económicas y políticas internacionales, y en algunos Estados acaparan un poder casi definitivo, al punto de dirigir la política económica e imponer a los gobiernos sus decisiones, a partir de una concepción doctrinaria conocida como neoliberalismo, que impone una organización económica internacional en la que la libre circulación de mercancías y los flujos financieros no encuentren el mínimo obstáculo para rentabilizar el capital, por lo tanto, esta conducta empresarial intenta impedir que los Gobiernos puedan realizar cualquier política social contradictoria con las exigencias del mercado”.[[3]](#footnote-3)

Un aporte a esta noción podría ser muy útil. Si partimos de la base que la mayoría de los delincuentes informáticos son menores de edad, en la práctica se trata de personas que han nacido dentro de este contexto global o cuando se perfilaba, por lo tanto no se podía dejar de lado su definición.

Es imposible hablar de un término como globalización sin apelar a la cultura dominante en estos últimos treinta años, reconocida como posmodernismo.

**1.2 – Las características del posmodernismo**

Existen muchas definiciones de posmodernismo y discusiones teóricas de sus autores, pero en síntesis se trata de un “movimiento internacional contemporáneo extensible a todas las artes".[[4]](#footnote-4) El filósofo francés Gilles Lipovetsky *(La era del vacío, 1983)* reflexiona sobre este movimiento desde la moda y sostiene que desde los años 60, ésta es cada vez menos un distintivo de clase y tiende a ser más abierta, tendiente hacia lo efímero, la seducción y la diversificación del gusto. Según este pensador, el predominio de lo individual por sobre lo universal, la marcada carencia de proyecto histórico y el consumismo general conducen al surgimiento de un individualismo narcisista: “este individualismo corresponde a la descrispación de las posturas políticas e ideológicas y a la sobrevaloración concomitante de las cuestiones subjetivas" y señala que "windsurf, skate, alas delta, la sociedad posmoderna es la era del deslizamiento”[[5]](#footnote-5). La creciente autonomía del individuo y la aparición de una nueva solidaridad entre pequeños grupos acompañan una ética no fundada en esencialismos ni en el deber, sino minimalista y pragmática, que huye de los fundamentos transmundanos y metafísicos.

Otro francés, Jean Francois Lyotard *(La condición posmoderna, 1979),* considera el fenómeno posmoderno desde los medios de información, y entiende que su expansión y consiguiente facilidad de acceso a una inabarcable cantidad de material de origen aparentemente anónimo es parte de esta cultura, y contribuye a la disolución de los valores de identidad y de la responsabilidad personal”.[[6]](#footnote-6)

Tanto globalización como posmodernismo son el contexto donde se han instalado la tecnología y la ciencia, favoreciendo la aparición de la informática como totalizadora de estos fenómenos. Gran parte de las actividades cotidianas y especializadas pasan, de una manera u otra, por la informática. Tanto hardware como software han pasado de ser palabras especializadas de la ciencia informática para señalar a la maquinaria como a los programas, respectivamente. El conjunto en su más amplio desarrollo y connotación, con la aparición de la red de comunicaciones Internet, ha formalizado la existencia de la virtualidad.

**1.3 – La virtualidad**

Desde un punto de vista técnico se llama realidad virtual a "la simulación por computadora, dinámica y tridimensional, con alto contenido gráfico, acústico y táctil, orientada a la visualización de situaciones y variables complejas, durante la cual el usuario ingresa, a través del uso de sofisticados dispositivos de entrada, a "mundos" que aparentan ser reales, resultando inmerso en ambientes altamente participativos, de origen artificial".[[7]](#footnote-7) Este tipo de definiciones abundan en la red Internet, y se caracterizan por la complejidad de datos que incorporan, la mayoría relacionados con la misma informática, y la aparición de un lenguaje especializado que sólo los programadores informáticos conocen con exactitud. Este lenguaje podría ser considerado como un "argot" o “jerga”, que comenzó a ser utilizado por usuarios o consumidores de informática no especializados académicamente en el tema, sino por curiosidad, obligación o como hobby.

En otros términos, podemos tomar la definición de virtualidad propuesta por la doctora Andrea Sarra, en su libro “Comercio electrónico y Derecho”, donde explica que "lo virtual constituye una fantasía, una representación onírica de la realidad o una alucinación", advirtiendo que "de hecho, en ocasiones, éstas pueden llegar a experimentarse tan vívidamente que no se puedan discernir de la realidad, o bien, en otras palabras, virtual es todo aquello que, sin ser real, aparece frente a quien lo contempla como si lo fuera".[[8]](#footnote-8)

Un ejemplo esclarecedor de virtualidad lo representa el uso de simuladores de vuelo para los pilotos. A partir del uso de una cabina real, a escala 1:1 se generan situaciones habituales de conducción y otras de riesgo, armadas por computadoras. Por lo general, estos simuladores sirven tanto para capacitar como para evaluar. La evaluación resulta así mucho más completa y precisa que una gestión similar realizada por humanos, por lo tanto el control queda totalmente en manos de una máquina aparentemente inteligente. No todas las personas se adaptan a estos sistemas de evaluación.

Actualmente, suele considerarse a la virtualidad como una consecuencia del mundo flexible e intangible de lo digital, del mundo de las redes, en suma, del mundo creado por la tecnología informática. E incluso los conceptos “virtual” y “digital” parecen ser patrimonio exclusivo de la segunda mitad del siglo XX. En rigor de verdad, la génesis de estas nociones no se encuentran en este siglo y la relación de correspondencia que hoy presentan no se ha mantenido históricamente.

En un sentido amplio, la realidad virtual, esa certidumbre cuya insuficiencia sólo es garantizada por su presunta inmaterialidad, habita en todos los recodos de la experiencia cotidiana. Se encuentra en los juegos del niño, en el sueño y en el soñar despierto.

También habita en la página escrita, en el espejo, en la pantalla de la TV y en la palabra misma, es decir, en el lenguaje. Por último, podemos considerar que son virtuales nuestro pensamiento y nuestra memoria.

La noción de virtualidad, para Sarra, "ha existido desde que los primates con rasgos antropomórficos adquirieron capacidad simbólica, por lo que sus orígenes se remontan, en realidad, hasta la prehistoria, cuando las pinturas rupestres de Altamira constituyeron el mundo virtual de sus creadores; mientras que en la antigüedad clásica, Platón, con su “alegoría de la caverna”, se refiere a la existencia de un mundo ideal (¿un mundo virtual?) distinto del real; por su parte la “mímesis” de Aristóteles, inducida en un público, generaba la “catarsis”, que era la capacidad de simulación emocional que habilitaba a los espectadores a entrar en empatía con los actores en el escenario e internalizar los dramas, con lo cual se producía un mundo virtual compartido: el drama".[[9]](#footnote-9)

Para la autora, en el mundo moderno "la realidad de la demostración científica de Galileo sucumbió ante el mundo virtual creado por la Inquisición en el oscurantismo; y más tarde, con el surgimiento de la comunicación masiva, la imprenta, la telegrafía, la telefonía, la radiofonía, la cinematografía, la televisión y el teleprocesamiento multimedial (computadoras y telecomunicaciones), la virtualidad se evidenció aún más".[[10]](#footnote-10) De esta manera nos hemos instalado en el punto ideal para reconocer de qué manera la tecnología ha insertado al ser humano, junto con las ideas dominantes posmodernas, tales como el individualismo, el hedonismo, el narcisismo, el consumismo, el nihilismo, en el mundo conocido como ciberespacio.

**1.4 – El ciberespacio**

Tanto los términos "cibernética" como "ciberespacio", muy utilizados en el lenguaje cotidiano, tuvieron su origen en el siglo XX dentro del conjunto de denominaciones propias de la tecnología, aunque sus primeros usuarios procedieran de diferentes ámbitos del saber.

Según Sarra, la palabra cibernética fue acuñada modernamente por el matemático norteamericano Norbert Weiner (1884-1964), a la que definió como "la ciencia dedicada al estudio de los métodos de comunicación y control, comunes a las máquinas y a los organismos vivos".[[11]](#footnote-11) Marie Ampére (1775-1836) el fundador de la electrodinámica designó con este nombre a la ciencia dedicada al control de la sociedad; al igual que el psicólogo estadounidense Burrhus Frederick Skinner (1904-1990).

Sin embargo, en la antigüedad, la expresión ya había sido utilizada por Platón para describir la ciencia que se ocupaba del control de la navegación de los barcos y, más tarde, para describir la ciencia o arte de la que las personas podían valerse para preservar sus cuerpos y riquezas de los peligros que les acechaban. Mucho más tarde, en el siglo XIX, André Heidegger habla de la cibernética como una especie de culminación de la filosofía.

Por su parte, el término ciberespacio toma su nombre del contexto formado por el prefijo de la palabra "cibernética", donde "cyber" se relaciona con todo lo que tiene conexión a robots y computadoras. El ciberespacio se refiere al ámbito donde transcurre la acción de los personajes de la novela de fantasía científica Neuromancer, ["Neuromante", en castellano] escrita por el canadiense William Gibson, en 1984.[[12]](#footnote-12) El autor ha descrito al ciberespacio como "un espacio indefinido que circunda la computadora y donde el ojo de la mente puede impregnarse y fusionarse en una alucinación consensual".[[13]](#footnote-13)

Este particular mundo virtual que se ha generado a partir de la tecnología de la información, el “ciberespacio”, para Sarra se trata "de interacciones interpersonales que se desarrollan en un particular espacio-tiempo, creando una nueva dimensión en la que no existe la limitación de la materia y el condicionamiento espacial.”[[14]](#footnote-14)

Por obvio que parezca, la tecnología de la información tiene por soporte la utilización de las computadoras. Es a partir de este avance que el mundo virtual es una réplica del real, que es en el que vivimos, donde asistimos a sus fortunas, sus miserias y que hereda todas sus desgracias pero también sus aciertos. Esta tecnología imperante tuvo su origen y desarrollo a partir de lo digital.

**1.4.1 - La noción de lo digital**

La noción de digital aparece alrededor de 1860 con la tecnología que comienza a perfilarse a partir de la electricidad. Uno de los primeros inventos, a partir de la posibilidad de conducir energía por cable, fue el telégrafo y la creación de un sistema de letras codificadas a puntos y rayas. Basándose en los descubrimientos de Ampère el estadounidense Samuel Morse (1791-1872) inventó el primer telégrafo eléctrico en 1843. Junto con el aparato ideó el Código Morse que rápidamente fue adoptado por todos los telegrafistas del mundo. El sistema incluía un aparato codificador en un extremo de la línea y otro, decodificador, en la otra, o en el segmento intermedio al que llegara el tendido. Lo importante aquí es señalar la utilidad de la manipulación, que recibió el nombre de digitabilización, pues el pulsado se realizaba con el dedo índice.

Sin embargo, con el tiempo el sistema se modernizó hasta llegar a los actuales medios de telecomunicaciones, que a nivel informático mantuvieron el lenguaje binario, traducido ahora como una convención entre ceros y unos (0 y 1).

Si uniéramos todos los apartados de este capítulo, hasta ahora, se hace evidente que toda la humanidad está integrada al ciberespacio. La tecnología ha suministrado los instrumentos de comunicación más sofisticados de la historia que son manipulados por cualquier ser humano. Pero, desde luego que también esto ha dado lugar a la aparición de consumidores especializados y no tan especializados, aunque sabemos que existen millones de personas que no tienen ningún contacto con esta tecnología, pero dependen de ella. En realidad la actitud que toman es la de no asumir el avance tecnológico, manteniéndose al margen de este avance cualitativo de la humanidad.

Ahora bien, los consumidores especializados y no tan especializados tienen conocimiento de la existencia de una virtualidad de lo digital.

**1.4.2 – Virtualidad de lo digital**

Lo digital como mecanismo creativo de un lenguaje diseñado para la manipulación de datos procesados por computadoras es patrimonio de un mínimo de especialistas. Todo el resto de los usuarios intuyen sobre el tema, pero desconocen cómo se hace, cómo se organiza, cómo funcionan los programas. Lo digital es real para los especialistas y virtual para los consumidores. Los primeros poseen los comandos e instrucciones para comunicarse con las máquinas y crear programas a partir de ello, pero los consumidores, por más especializados que sean, no necesitan conocer el origen de un programa, sino si se adapta a sus necesidades y deseos.

La relación existente con la tecnología implica un reducido número de especialistas en informática y el resto de la humanidad que son los usuarios de los bienes que generan los primeros.

El concepto mayor del avance tecnológico de lo virtual y lo digital lo representa la generación de redes comunicacionales, que por sutiles no dejan de ser reales.

Es importante tener presente que para el consumidor especializado lo virtual es real, o lo cree. Este consumidor ha logrado especializarse en redes y sistemas a partir de la disposición de tiempo y su ávida curiosidad. Generalmente quienes reúnen estas características son los niños y los adolescentes.

A lo largo de la historia de la humanidad los avances científicos y tecnológicos fueron utilizados por los distintos sistemas u organizaciones para facilitar sus tareas, fueran de organización, ejecución o control. Los ejemplos son infinitos. Todas las actividades humanas, por complejas que sean, han apelado a los cambios producidos por la ciencia y la tecnología.

Hoy no existe ninguna tarea humana que no pueda ser trasladada a la informática. Desde luego que este avance también ha incorporado a la virtualidad de lo digital actividades que requieren alto grado de privacidad. Los sistemas de seguridad se han desarrollado de la misma manera que los sistemas utilizados para cosas banales o públicas. A nivel de apreciación se podría decir que en esta virtualidad interactúan con idénticos orígenes lo serio y lo lúdico, lo estratégico y lo común, lo importante y lo accesorio, lo público y lo reservado o privado.

**1.5 – La convivencia con la tecnología**

El conjunto de datos aportados hasta aquí intentan dar forma al ámbito donde se sustenta esta investigación. Pero es necesario agrupar un conjunto de definiciones para integrar todos los conceptos e intentar la organización de un todo donde transcurren las acciones de aquellas personas que cometen delitos informáticos; porque se trata de individuos que "habitan" en este dominio.

El uso contemporáneo del término virtual proviene de la ingeniería de los programas (*software*) de computadoras. Los científicos del campo de las computadoras frecuentemente utilizan el término "memoria virtual" para describir la memoria de trabajo temporal *Random Access Memory* (RAM). Esto equivale a la memoria principal de trabajo de una computadora, en la cual se guardan instrucciones y datos de programas para que la unidad central de procesamiento (CPU) pueda acceder a ellos directamente a través del bus de datos externo de alta velocidad.

A la RAM se le conoce como memoria de lectura/escritura, para diferenciarla del otro componente de almacenamiento principal de una computadora, llamada "memoria ROM" de solo lectura [la *Read Only Memory* es la parte del almacenamiento principal de una computadora, que no pierde su contenido cuando se interrumpe el flujo de energía eléctrica. Contiene programas esenciales de sistema que ni el usuario ni la computadora pueden borrar. Como la memoria interna está en blanco al encenderla, la computadora no puede ejecutar ninguna función a menos que se le proporcionen las instrucciones de arranque.

Estas instrucciones se guardan en la ROM]. En la RAM, la CPU puede escribir y leer. La mayoría de los programas destinan parte de la RAM como espacio de trabajo temporal para guardar datos, lo que permite hacer (re-escribir) las modificaciones necesarias hasta que la información esté lista para imprimirse o guardarse en un medio de almacenamiento secundario, se trate de un disco flexible, o duro.[[15]](#footnote-15) La información se mantendrá flotante, "virtual" mientras no sea impresa.

Cada vez que se utiliza la palabra "virtual" se hace referencia a una realidad que no es formal, que no es una realidad "bona fide" (Helsel & Roth, 1991). Cuando describimos el "ciberespacio" o la realidad virtual como un espacio virtual, no definimos un espacio actual, sino algo que existe (de forma concreta o física) y contrasta con el espacio real o físico, pero que opera como si estuviese en un espacio real (Heim, 1991). Por otro lado, Osberg (1997) le resta un poco de importancia a la relación metafórica que se ha realizado con el espacio cibernético y el espacio real, resaltando que "el ciberespacio no es un lugar sino una experiencia".[[16]](#footnote-16)

Existe un sinnúmero de definiciones acerca de lo que conocemos como "realidad virtual". Esto se debe a la diversidad de aspectos a los que se puede aplicar esta tecnología.

Si partimos de lo básico, el diccionario define la palabra realidad como "la cualidad o estado de ser real o verdadero". Por otro lado, define la palabra virtual como "que existe o resulta en esencia o efecto pero no como forma, nombre o hecho real". La palabra virtual proviene del lenguaje medieval en Europa. Duns Scotus (quién murió en 1308) dio a este término una connotación tradicional. La palabra en latín "*virtualiter*" sirve como pieza central en su teoría de la realidad. Mantiene el concepto de las cosas que contienen un atributo empírico que no sustenta un aspecto formal, como si las cosas conocidas estuviesen aparte de la observación empírica (Heim, 1991).

La realidad virtual, como concepto neo-tecnológico, ha sido definida de varias maneras (Facultad de Ingeniería, UNAM, 1997):

“como un entorno en tres dimensiones sintetizado por computadora en el que varios participantes acoplados de forma adecuada pueden atraer y manipular elementos físicos simulados en el entorno y, de alguna manera, relacionarse con las presentaciones de otras personas pasadas, presentes o ficticias o con criaturas inventadas”.

“como un sistema interactivo computarizado, tan rápido e intuitivo, que la computadora desaparece de la mente del usuario, dejando como real el entorno generado por ella, por lo que puede ser un mundo de animación en el que nos podemos adentrar”.

Otros definen la "realidad virtual" como un ambiente interactivo generado por computadora, donde imágenes virtuales pueden interactuar mediante procesos especiales y modalidades no-visuales, tal como auditiva, táctil, entre otras, y así "convencer" al usuario de que está inmerso en un espacio sintético (generado por computadora) (Ellis, 1994, citado en North, North & Coble, 1996).

Una definición un poco más práctica es la que entiende la "realidad virtual" como aquella forma de trabajo en la que el ser humano puede interactuar totalmente con la computadora, generando espacios virtuales donde es posible desempeñar tareas y donde puede comunicarse con la máquina a través de dispositivos periferales o "equipos de interacción" tales como cascos o guantes (North, North & Coble, 1996; Fac. de Ingeniería, UNAM, 1997).

Es un mundo de objetos tridimensionales los cuales pueden ser observados, escuchados, y tocados (Browning, Cruz-Neira, Sandin & DeFanti, 1993). Utilizando estos "equipos de interacción", *"head mounted display"*, *"dataglove"*, el usuario puede visualizar e inclusive, "entrar" en un espacio virtual creado por computadora, una realidad alternativa donde el sujeto participa activamente (Sheneman, 1997).

Podemos sintetizar la definición de realidad virtual a "una forma en que el ser humano visualiza, manipula e interactúa con las computadoras y con datos extremadamente complejos" (Isdale, 1993).

Desde el punto de vista informático podríamos disponer de tantas “realidades” como quisiéramos. La generación del ciberespacio y la realidad virtual han creado la posibilidad de diluir y enmascarar nuestra identidad, e incluso multiplicarla a discreción según la conveniencia y los propósitos.

**Capítulo II**

**Las redes: la red Internet**

**2.1 – ¿Qué se entiende por red?**

La doctora Andrea Sarra incluye en su obra una definición muy apropiada de red informática, considerando que se trata de "un conjunto de computadoras interconectadas entre sí a los efectos de compartir recursos tales como información, discos, impresoras, módems".[[17]](#footnote-17)

Una red tiene tres niveles de componentes: software de aplicaciones, software de red y hardware de red.

El software de aplicaciones está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).

El software de red consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

El hardware de red está formado por los componentes materiales que unen las computadoras.

Una red es estable cuando no se colapsa y permite que las actividades prosigan sin interrupciones. La lógica de la red exige una optimización constante a través de la conexión y desconexión de los recursos según lo que se necesita en cada caso, con la única limitación de la necesidad de estabilidad.[[18]](#footnote-18)

La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

La red es un canal o medio material por el que transita la información y es justamente esto, la información, el verdadero valor que encierra Internet. Por ello se suele pensar a la red Internet como una “autopista de la información”.

La red Internet es una nueva infraestructura de aprendizaje, ya que ofrece toda clase de cosas, desde enciclopedias, pasando por cursos universitarios, programas de formación interactivos sobre diversos temas, grupos académicos de debate, o acceso a las bibliotecas del mundo, hasta información sobre cómo cuidar un perro enfermo.[[19]](#footnote-19)

**2.2 – El origen de la red Internet y la cultura hacker**

Son variados los intentos por definir a la red Internet. En esta investigación se ha tomado la definición del "Diccionario de computación e Internet", que dice que se trata de "un sistema de redes de computadoras enlazadas, con alcance mundial y de continuo crecimiento, que facilita servicios de transmisión de datos como el inicio de sesión remoto, transferencia de archivo, correo electrónico, World Wide Web y grupos de noticias [...] Internet descansa sobre TCP/IP (un protocolo de control de transmisión) que asigna a cada computadora conectada una dirección Internet única, conocida también como dirección IP, con el fin de que dos computadoras conectadas puedan localizarse entre sí en la red para cambiar datos.

Los servidores que forman cada una de las redes están diseminados por todo el mundo y enlazados a Internet por una variedad de caminos de alta capacidad o de gran ancho de banda (fibra óptica, satelital), de capacidad media (cable coaxil) y de baja capacidad o ancho de banda pequeño (línea telefónica convencional). A su vez, cada una de las computadoras personales de los usuarios está conectada al sistema por intermedio de módems (Modulador-Demodulador), que son dispositivos que conectan las líneas telefónicas, las líneas de cable o la fibra óptica a las computadoras personales.

Cuando una computadora está conectada a una red, realiza una función básica esencial: la de compartir recursos, tanto de hardware (discos, impresoras, scanners, etc.) como información (software, datos, documentos). Inicialmente, las redes eran utilizadas fundamentalmente para compartir recursos de hardware y para el almacenamiento de archivos a los cuales los usuarios podían acceder. Actualmente estas funciones han evolucionado para convertirse en servidor de una base de datos *(data base server)* y un servidor de aplicaciones *(application server).*

Aunque existen conexiones de Internet en prácticamente todos los países, el idioma predominante en la red es el inglés. La mayoría de los usuarios viven en países angloparlantes, donde la red es vista como un nuevo medio de comunicación pública, potencialmente a la par con el sistema telefónico o la televisión por su ubicuidad e impacto".[[20]](#footnote-20)

La red Internet como fenómeno científico abarca a todas las actividades humanas en esta parte del tiempo histórico, favoreciendo la conformación de una cultura, que surge a partir de la acción sostenida de los investigadores y científicos norteamericanos formados a partir de la posguerra, en 1945.

Esta cultura se sostiene en un conjunto de necesidades de gobiernos y empresas para mejorar las comunicaciones, y apelan a la informática para utilizarla como medio. Esta posibilidad entusiasmó a los investigadores más jóvenes. La informática siempre atrajo a los más jóvenes por muchas razones, pero en principio creo que es porque se trata de un trabajo que se hace como jugando.

En pocas oportunidades en la historia lo lúdico, lo científico y lo técnico se han unido de la forma en que se ha hecho posible en la segunda mitad del siglo XX. Estos jóvenes investigadores, en su actividad conjunta crearon bloques de trabajo, interconectados con incipientes redes, constituyendo grupos de cultores informáticos y con esta práctica comenzó a perfilarse la cultura hacker.

Los principios de la cultura hacker tal y como la conocemos hoy en día pueden ser convenientemente datados a partir de 1961, año en el cual el *Massachusetts Tecnological Institute*  (MIT) adquirió su primer ordenador PDP-1. El comité de señales y potencia del Club Tecnológico de Modelos de Ferrocarril adoptó la computadora como su juguete tecnológico favorito e inventó las herramientas de programación, la jerga y una cultura entera circundante que es reconocible por nosotros hoy en día. Estos primeros años han sido examinados en el libro de Steven Levy *"Hackers".*

La cultura computacional del MIT parece haber sido la primera en adoptar el término "hacker''. Los *hackers* del Club Tecnológico de Modelos de Ferrocarril se convirtieron en el núcleo del *Laboratorio de Inteligencia Artificial* del MIT, el centro líder mundial en Inteligencia Artificial (IA) durante los primeros años 80.

Su influencia se extendió más allá de 1969, el primer año de ARPANET. El territorio hacker floreció en las universidades conectadas a la red, especialmente -aunque no exclusivamente- en sus departamentos de ciencias de la computación. Los primeros artefactos intencionales de la cultura hacker -las primeras listas de argot, las primeras sátiras, las primeras tímidas discusiones de la ética hacker- todo ello fue propagado en Arpanet en sus primeros años.

En particular, la primera versión del diccionario especializado, que recibió el nombre de "Jargon File", en español archivos de jerga, fue desarrollada a través de una intrincada colaboración durante 1973-1975. Este diccionario de argot se convirtió en uno de los documentos definitorios de la cultura. Fue eventualmente publicado como "The Hacker's Dictionary" en 1983. Una versión corregida y aumentada es el "New Hacker's Dictionary".[[21]](#footnote-21)

La primera red de ordenadores transcontinental de alta velocidad la produjo ARPANET (Advanced Reserch Project Agency Network), construida por el Departamento de Defensa de los Estados Unidos como un experimento de comunicaciones digitales, pero creció para unir los cientos de universidades, contratistas de defensa y los laboratorios de investigación. Esto permitió a investigadores de cualquier parte de EE.UU. intercambiar información con una velocidad y flexibilidad sin precedentes, dando un avance hacia el trabajo colaborativo e incrementando enormemente tanto la velocidad como la intensidad del desarrollo tecnológico.

La Fundación Nacional de Ciencia de los EE.UU. construyó su propia red (NSFnet) usando tecnología IP. Esta conectó los centros más importantes del país con cadenas locales alrededor de cada nodo.

Este modo de conectividad se llama *rizomático,* de rizoma, el tallo es visible, pero penetra en la tierra para formar una nueva planta, sustentada por el conjunto para crecer y extenderse.

Así, la red NSFnet se unió a la red ARPANET, y nació Internet, unificando pequeñas redes. El nombre Internet proviene de los vocablos anglosajones ***Inte****rnational* ***Net****work of Computers,* en español, Red Internacional de Computadoras.[[22]](#footnote-22)

Durante una década, creció a un ritmo constante, y por el abaratamiento de los costos de las comunicaciones y del hardware, aparecieron las PC (Personal Computer) no sólo para uso empresarial o laboral, sino como entretenimiento doméstico. Así en poco tiempo se incrementó el uso de Internet y se extendieron sus alcances por la aparición de los usuarios públicos.

El soporte de la información en la incipiente red, recibió el nombre de sitios, que luego adoptaron el nombre genérico de WEB, identificando así su composición similar a una telaraña. En general los sitios de la red Internet se formalizan bajo la sigla WWW, equivalente a World Wide Web, y su traducción al español por "amplia telaraña -de redes-global".

El auge de Internet surgió en 1993 con el lanzamiento de Mosaic, el primer navegador gráfico, creado por Marc Andressen, que contribuyó a la enorme difusión de la World Wide Web. Este programa de computadoras permitía ir de un lugar a otro dentro de la red de Internet en un entorno gráfico, sin necesidad de escribir complicados códigos, sino señalando sencillamente con el ratón o mouse un icono, que es una imagen que representa un programa u otro recurso; un gráfico o una palabra o lo que se decidiera visitar.

En la actualidad Mosaic, así como sus sucesores, el actual Netscape Navigator o Internet Explorer permiten que con sólo hacer un clic con el mouse en algunas palabras y figuras, llamados en Inglés *hyperlinks* (hipervínculos) el navegador lea automáticamente páginas en cualquier computadora conectada en el WWW, naciendo con esto la palabra que hoy conocemos como "navegar".

A finales de los años 90, el desarrollo de Linux y la ideología de Internet se convirtieron en las principales actividades de los *hackers*. La World Wide Web convirtió Internet en un medio de masas, y muchos de los *hackers* de los años 80 y de principios de los años 90 lanzaron los proveedores de servicios de Internet, vendiendo o dando acceso a las masas.

La ideología de Internet llevó incluso a la cultura hacker a los inicios de la respetabilidad y de aspiraciones políticas. En 1994 y 1995 el activismo hacker arruinó la propuesta Clipper que pretendía poner la encriptación fuerte bajo el control del gobierno norteamericano. En 1996, algunos *hackers* movilizaron una amplia coalición para vencer la mal llamada "Acta de Decencia de las Comunicaciones" ya que presintieron la censura en Internet.

En la actualidad, Internet trata de ser el medio de comunicación social más democrático conocido, aunque todo el proceso de codificación siempre se mantenga dentro de los límites generados por los administradores de la red.

**2.2.1 – Origen del término hacker**

El término *hacker* es una expresión idiomática inglesa cuya traducción literal al español tiene varios significados, siendo el más popular el atribuido a "una persona contratada para un trabajo rutinario", y que por la naturaleza del mismo es tedioso, entregado, y hasta maniático.

El apelativo de hacker se crea a fines del siglo XIX cuando los Estados Unidos de América empiezan a recibir un masivo movimiento migratorio de personas de todos los países del mundo, que esperaban encontrar en el "país de las oportunidades", un bienestar económico y progreso.

Los hackers eran trabajadores informales de la estiba que se pasaban todo el día bajando maletas y bultos de las personas y familias completas que llegaban en barcos a los puertos de Nueva York, Boston, San Francisco. Estos trabajadores eran infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero. La palabra "hack" en inglés significa "hacha" en español. Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La palabra hacker aplicada a la informática se refiere a las personas que se dedican a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía.

El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen un desarrollado sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos.

"La revolución de la computación ha sido lograda gracias a los hackers", afirman categóricamente los estudiosos e investigadores pioneros de los virus de computadoras Rob Rosenberg y Ross Greenberg. Según ellos, “un hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, sólo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental. Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa”.[[23]](#footnote-23)

Hacker, originalmente, un aficionado a los ordenadores o computadoras, un usuario totalmente cautivado por la programación y la tecnología informáticas. En la década de 1980, con la llegada de las computadoras personales y las redes de acceso remoto, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar o alterar los programas o los datos almacenados en las mismas. También se utiliza para referirse a alguien que, además de programar, disfruta desmenuzando sistemas operativos y programas para ver cómo funcionan.

Según la definición de Sarra “un hacker es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas".[[24]](#footnote-24)

Se considera que hay dos tipos: 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables”[[25]](#footnote-25).

El hacking se considera una ofensa o ataque al derecho de gentes, y no tanto un delito contra un Estado concreto, sino más bien contra la humanidad. En general los hackers son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo, pero también todos saben que se trata de individuos de nivel inteligente superior y de gran capacidad laboral.

Existe una serie de grupos dedicados al hacking que se extiende a través de la red Internet y por este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización.

Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectara a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas.

En España hay ejemplos recientes, como es el caso de Hispahack, que realizó ataques a varios sistemas, incluidos los de algunas universidades. También se ha creado en la Guardia Civil un grupo especializado en todo tipo de delitos informáticos para identificar e investigar a estos modernos delincuentes.

**2.2.2 – Algunas definiciones asociadas**

La idea que se tiene sobre la cultura hacker es vaga, porque en innumerables casos se incluye al término generalizando, pero a medida que las actividades de los mismos se han ido especializando, también han surgido los nuevos términos. A continuación se incluye un repertorio de definiciones obtenidas del diccionario de términos informáticos, que ilustrarán someramente el universo de la cultura hacker.

HACK: 1. Nueva disposición inteligente y poco usual de los recursos existentes del sistema o red que produce, como por arte de magia, una mejora notable en el rendimiento del sistema, o una jugarreta casi igual de sorprendente. Un hacker es quien usa las computadoras para producir estos efectos y no es, necesariamente, un criminal informático. 2. Un trabajo “rápido y práctico” que produce resultados, pero sin seguir ningún procedimiento lógico u ordenado.

HACKER: 1. Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación o red y, mediante una programación hábil, llevar el sistema al nivel máximo de rendimiento. 2. La prensa lo utiliza como sinónimo de cracker. 3. Programador experto.

CRACK: Aficionado a la computación que disfruta acceder sin autorización a sistemas de computación. Esta actividad es un juego pretencioso y tonto, cuyo fin es derrotar inclusive a los sistemas más seguros. Aunque muchos crackers hacen más que sólo dejar una “tarjeta de presentación” para probar su hazaña, algunos intentan robar información de tarjetas de crédito o destruir información. Cometan o no un delito, todos los crackers perjudican a los usuarios legítimos de los sistemas ocupando tiempo de los administradores del sistema y dificultando el acceso a los recursos del sistema. En la prensa el término “cracker” se utiliza como sinónimo de “hacker”, pero esta última actividad tiene un significado completamente diferente y desempeña un papel importante en la computación.

HACKER ETHIC-ETICA DEL HACKER: Conjunto de principios morales que fueron comunes a la primera generación de la comunidad de hackers (alrededor de 1965-1982), descrita por Steven Levy en *Hackers (1984).* De acuerdo con la ética del hacker, toda la información técnica debería, en principio, estar a la disposición de todo el mundo, de modo que no es inmoral entrar a un sistema para explorarlo y obtener más conocimiento. Sin embargo, siempre es inmoral destruir, alterar o mover datos de tal forma que cause daños o gastos a otros.

**2.3 - La ética del hacker**

Los términos que relacionan la ética en informática reciben el nombre de Nética y Netiqueta, como figura y fondo de un problema. El primero, que incluye a la ética en la red y la segunda, como las acciones que pueden incluirse dentro del primer concepto.

La expresión Nética alude a la relación que el hacker mantiene con las redes de nuestra actual sociedad red en un sentido más amplio que el término más habitual de netiqueta -que concierne a los principios de conducta en el contexto de la comunicación en Internet, por ejemplo, “evitar expresiones inadecuadas”, “leer el archivo de preguntas mas frecuentes antes de enviar un mensaje”, y otros-. No todos los hackers, por supuesto, comparten la integridad de los elementos de esta nética; no obstante, estos elementos en su conjunto se hallan ligados en cuanto a su significado y relación social con la ética del hacker.

Tal relación se remonta al origen de la ética hacker en la década de 1960, la nética ha recibido una formulación más consciente en los últimos años. Un momento esencial en esta formulación tuvo lugar en 1990, cuando los hackers Mitch Kapor y John Terry Barlow pusieron en marcha la Fundación Frontera Electrónica (EFF), en San Francisco, con la finalidad de potenciar los derechos del ciberespacio.

Barlow fue el primero en aplicar el término ciberespacio, creado por William Gibson en su novela “Neuromante”, a todas las redes electrónicas. Kapor fue una importante figura en el desarrollo de los ordenadores personales, al crear, en 1982, el programa de hoja de cálculo Lotus. El término Lotus refleja el origen cultural de Kapor, como licenciado en Psicología y asesor en cuestiones de salud mental, y más tarde instructor de meditación trascendental, mostró un gran interés por los sistemas orientales de pensamiento.

Tanto Barlow como Kapor consideraron cuestiones de primera importancia los derechos fundamentales del ciberespacio, como la libertad de expresión y la privacidad.

La EFF se define como una “organización sin ánimo de lucro y no partidista, que trabaja en defensa del interés publico para proteger las libertades civiles fundamentales, entre ellas la privacidad y la libertad de expresión, en el ámbito de la informática e Internet”.

Concretamente “la EFF ha contribuido a invalidar, entre otras medidas, la *Comunication Decency Act* aprobada por el Congreso de EE.UU en 1997, cuya finalidad era crear una especie de autoridad en Internet.

La EFF ha desempeñado también un papel destacado en la defensa de la utilización de las tecnologías de fuerte encriptación que habían sido declaradas ilegales con anterioridad en EE.UU.

La necesidad de la existencia de organizaciones de hackers, como la EFF, surgió cuando, en la década de 1990, gobiernos y empresas se interesaron a gran escala por Internet y, desde entonces, han intentado a menudo conducirla en dirección opuesta a los ideales hackers.

En su defensa de la libertad de expresión y la privacidad, el mundo hacker se muestra casi siempre descentralizado. Además, de la EFF existen muchos otros grupos hackers comprometidos en una actividad similar. Dos ejemplos de ello son el servicio de Internet XS4ALL y Witness, con sede en Holanda, cuyo compromiso ético les lleva a editar informes sobre los crímenes contra la humanidad utilizando las herramientas del ciberespacio.

Estos grupos de hackers unen fuerzas en colectivos temáticos como la *Global Internet Liberty Camping”*.[[26]](#footnote-26)

Según Steven Levy en su libro 'Hackers', desde el principio los hackers originales desarrollaron un código de ética o una serie de principios que simplemente eran tomados como un acuerdo implícito y no como algo escrito o fijo.

Este código decía que "el acceso a las computadoras debe ser ilimitado y total", "el acceso a la información debe ser libre y gratuito", "desconfíen de la autoridad, promuevan la descentralización", "los hackers deben ser juzgados por su habilidad, no por criterios absurdos como títulos, edad, raza o posición", "se puede crear arte y belleza en una computadora", "las computadoras pueden mejorar tu vida".

Estas eran las premisas que aceptaban aún casi sin saberlo o sin expresarlo los hackers de los años sesenta.

Cómo fue evolucionando esta ética es difícil conocerlo, ya que se trata de fenómenos que están sucediendo a la velocidad de la luz y se torna complejo conocer los límites del ciberespacio por la cantidad de información existente, de usuarios, de lenguajes. Lo que se puede ver es que la red Internet se ha diversificado y extendido en treinta años a nivel mundial. Y en la hoy llamada aldea global, las cuestiones éticas fueron consideradas desde el comienzo por los primeros programadores y diseñadores de software animados a compartir, sin ser esto comprendido.

Ellos creyeron ser los verdaderos creadores de la red, esto es así desde el punto de vista que ellos fueron los “hackers”, esos trabajadores infatigables que desafiaban con su intelecto los límites del conocimiento y receptores de significativas sumas de dinero; pero su cultura se fue transmitiendo a través de las generaciones, deformando y siguiendo un curso hacia los hoy denominados delitos informáticos.

Algo que comenzó como un juego para algunos, se convirtió en el medio o instrumento delictivo para otros sujetos con ciertas características de personalidad y en un grave perjuicio para empresas, gobiernos y usuarios de Internet. Así las computadoras en sus manos, se convirtieron en un juguete muy poderoso y peligroso para terceros.

**Capítulo III**

**Los delitos informáticos**

**3.1-** **Concepto de delito**

En la actualidad la informatización se encuentra instalada en todos los países. Tanto en la organización y administración de empresas privadas o públicas, como en la investigación científica, en la producción industrial o en el estudio, e incluso en el ocio.

El uso de la informática es indispensable. Sin embargo, junto a las incuestionables ventajas que presenta para los usos comunes, comienzan a aparecer algunas facetas negativas, tales como la "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso o la utilización indebida de la información que puede afectar la esfera de la privacidad son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Estos hechos han propiciado la aparición de la contraparte, grupos cuya organización se han nutrido de las leyes generales de cualquier país, administrada, desde luego, por el Derecho, con la concurrencia interdisciplinaria necesaria para cualificar y sistematizar de alguna manera qué hacer ante esta nueva forma de delincuencia.

Todos los países, incluyendo el nuestro, han debido partir del concepto básico de delito, que implica una acción antijurídica realizada por una persona, tipificado, culpable y punible.

Si bien estos elementos de la definición son conocidos, a la hora de tipificar los delitos informáticos la línea que los determina no es muy marcada. Lo importante es que el Derecho para definir al delito informático se basó en los mismos principios del delito común.

Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial -estafas, apropiaciones indebidas, fraude-. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Los delitos informáticos, en gran parte, se hacen evidentes a partir del fraude, Pero, el fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud, y su relación con la definición de "delito", en este caso, puede ser más compleja, porque en principio el presunto delincuente no es real, es virtual. Si tomamos nuestra información precedente, connotaremos que se trata de una verdadera dificultad para tipificar al delincuente informático, porque sabemos que está allí pero no sabemos ni quien es, cómo es, ni siquiera dónde está ni de qué forma actuará a futuro, o si tomará una nueva forma o una nueva identidad.

Los estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquélla condiciona a ésta.

Según el Código Penal los elementos determinantes del delito son:

El delito es un acto humano, es una acción, se trate de acción u omisión.

El acto humano debe ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

Debe corresponder a un tipo legal –la figura de delito-, definido por La Ley, ha de ser un acto típico, por estar tipificado en el Código.

El acto ha de ser culpable, imputable a dolo (porque ha tenido intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

La ejecución u omisión del acto debe estar sancionada por una pena.

En un sentido jurídico, que indique las características de la acción amenazada con pena, podemos definir el delito "como acción típicamente antijurídica y culpable”.[[27]](#footnote-27)

**3.2- Concepto de delito informático**

El surgimiento de las redes internacionales informáticas, como Internet, permite a los usuarios entablar comunicaciones, actividades y transacciones con otras personas usuarias de toda la Aldea global.

Las agresiones en Internet reciben el nombre de ataques, estos se realizan contra algo medular: la información. A su vez, ésta puede sufrir distintos tipos de intromisión para agredirla en su confidencialidad o integridad.

“Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún. Sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización”.[[28]](#footnote-28)

Algunos autores sostienen que los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la Nación.

Se ha tratado de encuadrar los delitos informáticos dentro de los ya tipificados: robo, hurto, fraudes, falsificaciones, estafa, sabotaje.

Un elemento importante a tener en cuenta es que muchas veces el delito se va a convertir en un "caso internacional", ya que la información viaja sin tener en cuenta las fronteras de los Estados.

La Universidad de México ha realizado un estudio, y define a los delitos informáticos como "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, [...] que hacen uso indebido de cualquier medio informático".[[29]](#footnote-29)

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como "abarcante", al considerar al delito informático como "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".

Por su parte, el tratadista penal italiano Carlos Sarzara, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".[[30]](#footnote-30)

La abogada mexicana María de la Luz Lima concentra su definición en el concepto de *delito electrónico*, sosteniendo que "en un sentido amplio, es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel principal, ya sea como método, medio o fin".[[31]](#footnote-31)

En síntesis, aunque nuestro Código Penal no contempla una definición de los mismos, podría pensarse que un delito informático es una conducta que se verifica cuando la persona ingresa en forma ilegal en el equipo o sistema informático de otra invadiendo su privacidad. Provoca un daño a tal red o equipo, o la pérdida de la información contenida en los mismos, o modifica, destruye o copia tal información. Como en todos los delitos, el elemento subjetivo está constituido por el dolo o la culpa con que actúe el delincuente.

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora". "delincuencia relacionada con el ordenador".

**3.3 Características de los delitos informáticos:**

Según el abogado mexicano Julio Tellez Valdez, los delitos informáticos presentan las siguientes características principales:

“Son conductas criminales de cuello blanco (*white collar crime*), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

Son acciones ocupacionales, dado que muchas veces se realizan cuando el sujeto se encuentra en su trabajo.

Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Provocan serias pérdidas económicas, ya que casi siempre producen «beneficios» de más de cinco cifras a aquellos que las realizan.

Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

Son muchos los casos y pocas las denuncias

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

Ofrecen facilidades para su realización a los menores de edad”.[[32]](#footnote-32)

**3.4-** **Clasificación y descripción de algunos delitos según la actividad informática**

**3.4.1 Sabotaje informático**

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, derramar café o agentes cáusticos en los equipos).

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos, sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

- **Las bombas lógicas o cronológicas:** *(time bombs)* en esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador es identificado por el programa como la señal para empezar a actuar. La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa. Y así fue.

- Otra modalidad que actúa sobre los programas de aplicación es el llamado **«cáncer de rutinas»** *(«cancer routine»).* En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

- Una variante perfeccionada de la anterior modalidad es el ***virus informático****,* que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

- Los **gusanos**, *(worms)* se fabrican de forma análoga al virus; y se infiltran en los programas ya sea para modificar o destruir los datos, pero se diferencian de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo, un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruirá.

**3.4.2 Fraude a través de computadoras**

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. Esta forma de conducta se relaciona con la **manipulación de los datos de entrada (***input***)** en un sistema informático.

El abogado Ulrich Sieber, cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga -cómplice en la maniobra- mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, **alterando el programa o secuencia lógica** con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor.

A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

El nombre se debe al episodio de la Ilíada de Homero, Ulises urdió una estratagema en virtud de la cual le regala a los troyanos un gran caballo de madera, que en el interior ocultaba soldados, haciendo creer que el ejército griego abandonaba el sitio de la ciudad. El caballo entró en el recinto amurallado de Troya y aprovechando la noche y la confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad. Así, estas instrucciones paralelas actuarían en un sistema informático como los soldados escondidos en el caballo de Troya.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador, a esta modalidad se la conoce como **manipulación de los datos de salida (***output***).**

Una característica general de este tipo de fraudes, es que la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de «manipulación del programa», la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría llevar a cabo estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro (Ver Caso Nº 2).

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (depósitos monetarios, créditos).

En otros casos, los datos que motivan el fraude, representan objetos corporales (mercadería, dinero en efectivo) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles.

En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado» por el autor”.[[33]](#footnote-33)

Un ejemplo de uno de los métodos utilizados para realizar fraude a través de una computadora son los llamados *estratagemas.*[[34]](#footnote-34)

Los estafadores utilizan diversas técnicas para ocultar computadoras que se «parecen» electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos. El afamado pirata norteamericano Kevin Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad. (Ver Caso Nº 1)

***3.5 Otros delitos informáticos***

Además del sabotaje informático y el fraude hay variados tipos de delitos que se pueden realizar, a través del uso de una computadora en red; como las falsificaciones informáticas; las estafas; el acceso no autorizado a servicios y sistemas informáticos; la copia ilegal de software, la piratería de DVD y libros, entre otros. Pero hay también otros delitos convencionales, que con la aparición de las rutas virtuales se están reproduciendo también en el ciberespacio. Predominan:

- **Espionaje:** Se presentan casos de acceso no autorizado a sistemas informáticos e intercepción de correo electrónico de entidades gubernamentales, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, evidenciándose una vez mas la vulnerabilidad de los sistemas de seguridad gubernamentales por personas especializadas. (Ver Caso Nº 12)

- **Terrorismo:** La presencia de equipos que encubren la identidad del remitente, convirtiendo el mensaje en anónimo, los servidores que ofrecen servicio de correos gratis permitiendo ingresar datos personales y direcciones ficticias para crear cuentas de correo que posteriormente aprovecharon personas o grupos terroristas para enviar amenazas, remitir consignas y planes de actuación ilícitos.

- **Narcotráfico:** Utilizando mensajes encriptados para ponerse en contacto, se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. Al igual que los narcotraficantes, se presentan los traficantes de armas, las sectas satánicas, entre otros, obteniendo las mismas ventajas que encuentran en Internet, aprovechadas para la planificación de los respectivos ilícitos que se están trasladando de lo convencional al ciberespacio o viceversa.

- **Difusión de pornografía:** En la mayoría de países, así como en el nuestro, es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia.

- **Snuff:** Se trata de películas que muestran violencia y asesinatos reales.

En esta investigación no hemos entrado en esta temática relacionada con las perversiones, ya que sólo la hemos limitado a los casos de delitos de fraude a través de las computadoras.

**3.6 - Estadísticas sobre delitos informáticos**

Según el abogado argentino Pablo Palazzi en “todos los estudios, informes y estadísticas sobre delitos informáticos se encuentran dos temas comunes: además de tratarse de montos considerables, las cifras de defraudaciones por computadora cada año se incrementan”[[35]](#footnote-35).

Por ejemplo, Daniel Altmark señala que "el Instituto Suizo de Seguros ha informado que las compañías aseguradoras sufrían pérdidas anuales equivalentes a cuatro mil millones de francos emergentes de los denominados delitos informáticos. En Francia, en 1984, el resultado de los diferentes tipos delictuales vinculados a la informática, ascendió a la suma de setecientos millones de francos, la que en el mismo año, haciendo un estudio comparativo, equivalía a un monto diez veces mayor al emergente de los asaltos tradicionales a bancos efectivizados a toda Francia durante el mismo período".[[36]](#footnote-36)

Estas informaciones convalidan las necesarias estadísticas, de cuyos datos podemos determinar el grado de importancia del tema.

En los Estados Unidos, por ejemplo, el *Stanford Research Institute* detectó sólo diez delitos informáticos en el año 1969, pero en el año 1977 esa cifra subió a ochenta y cinco. (*Combating Computer Crime. Prevention, Detection, investigation,* Chantico Publishing Company, Inc., p.24.)

El *Computer Emergency and Response Team* de la Universidad de Carnegie-Mellon reportó desde 1991 a 1994, un 498 % de incremento de intrusiones informáticas, y 702 % de incremento en el número de sitios afectados. Durante 1994, por ejemplo, aproximadamente 40.000 computadores conectados a Internet fueron atacados en 2.460 incidentes. En igual sentido, el denominado *National Computer CrimeSquad del FBI* ha abierto más de 200 casos de hackers desde que fue creado en 1991.[[37]](#footnote-37)

Desde el año 2000, en los Estados Unidos existe una institución que realiza un estudio anual sobre la seguridad informática y los crímenes cometidos a través de las computadoras.

Esta entidad es el Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos", realizado a un total de 273 instituciones, principalmente grandes corporaciones y agencias del gobierno.

Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de Delitos Informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los delitos informáticos en los Estados Unidos de Norteamérica.

Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

**Violaciones a la seguridad informática**



El 10% de las respuestas no reportaron violaciones de seguridad, en cambio el 90%, sí. 90%

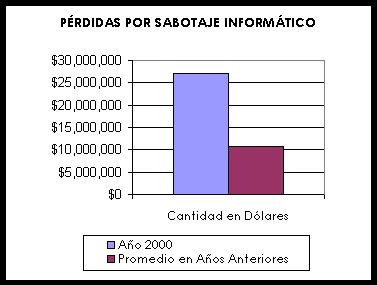
De las 273 instituciones encuestadas la mayoría descubrió violaciones a la seguridad de las computadoras dentro del último año.

El 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados, por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

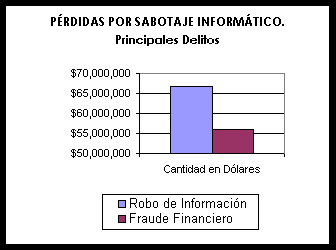
**Pérdidas financieras por sabotaje informático**

El 74% de las empresas encuestadas reconocieron pérdidas financieras debido a las violaciones de las computadoras.

Las pérdidas financieras ascendieron a U$S 265.589.940 (el promedio total anual durante los últimos tres años era U$S 120.240.180).



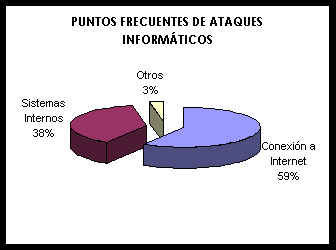
Un total parcial de 61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de 27.148.000 de dólares. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo U$S 10.848.850.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron U$S 66.708.000) y el fraude financiero (53 encuestados informaron U$S 55.996.000).

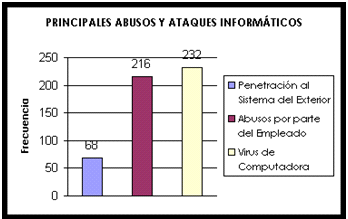
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

**Accesos no autorizados**



El 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades. Los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Los encuestados detectaron una amplia gama de ataques y abusos.

La "línea caliente" de la *Internet Watch Foundation* (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

En 2004, en la Argentina, el 23% de la población accede a Internet, con mayor penetración que México (11%) y Brasil, donde el 21% tiene acceso a la red. El 90% de los usuarios que navegan por la red la usan para comunicarse por e-mail o para el chat. Aunque nuestro país adoptó la red tiempo más tarde que otros países, su crecimiento ha sido mucho más acelerado. En términos generales, se debe tener presente que los países que son víctimas de ataques en primer lugar son los Estados Unidos y Brasil, mientras que los países en donde más se practica el hacking y sus variantes son China y también Brasil.

Algunos estudios prácticos demuestran que los hechos constitutivos de delincuencia informática, generalmente, pueden prevenirse .Se considera que el 90% de los delitos informáticos pueden ser evitados[[38]](#footnote-38).

**Capítulo IV**

**Estudios psicológicos de los delincuentes informáticos**

**4.1 – La psicología jurídica y su articulación con el delincuente informático**

Como vimos en el capítulo anterior, delito informático es el robo, adulteración, o hurto de herramientas o de información almacenada de forma digital. Si bien este tema está en discusión en varios campos de la ciencia, se pude generalizar que los siguientes son calificados como delitos informáticos:

Robar información.

Ingresar a una red ilegalmente.

Ver información no autorizada.

Pirateo de software (se está dañando propiedad intelectual)

Reproducción de música o DVD (se está dañando propiedad intelectual)

Los implementos para robar información son las computadoras conectadas en red, las telecomunicaciones. Predominan dos tipos de conductas: la que utiliza una herramienta informática, o bien las que atacan a las herramientas.

Estas conductas podrían comprenderse mejor teniendo en cuenta que constituyen delitos graves en la mayoría de los países, planteado desde el marco de la Psicología Jurídica, que según Del Popolo "es el estudio desde la perspectiva psicológica de conductas complejas y significativas en forma actual o potencial para lo jurídico, a los efectos de su descripción, análisis, comprensión, crítica y eventual actuación sobre ellas, en función de lo jurídico”.[[39]](#footnote-39)

El delincuente informático conoce la importancia que tienen los equipos, los sistemas y la información para la empresa. Accede en forma ilegal al sistema de la empresa y roba una base de datos; la roba porque la puede vender millones de veces sin dejar nunca de seguirla poseyendo; una vez robada, extorsiona a la empresa -a ningún inversionista le gustará enterarse a través de los periódicos que los sistemas informáticos de su empresa son fácilmente violables y a ningún cliente, el que sus datos de tarjetas de crédito, domicilio o número celular pueden estar circulando por ahí-.

Un delincuente informático modifica, sustrae o destruye la información o daña los sistemas informáticos como una manera de manifestarse contra la globalización o la guerra; otro, para vengarse de un despido; uno más, por la esperanza de que una vez probada su pericia tecnológica, sea contratado por el Director de IT de la empresa víctima del ataque; otros muchos, porque la empresa rival les ha pagado para infiltrar un virus, "tirar" la página Web del competidor (denegación del servicio) u obtener sus secretos industriales. Incluso la pura amenaza de soltar un virus puede ser una forma de extorsión lucrativa.[[40]](#footnote-40)

**4.2 – La psicología profunda y la comunicación**

La comunicación es un proceso que consiste en ser partícipes con una o más personas de ideas, sentimientos, propósitos o creencias. Es el producto de un cambio y promotora de nuevos cambios.

David Liberman consagró su vida a la música y luego al psicoanálisis y de alguna manera logró integrar ambas esferas o disciplinas, ya que además de su aplicación de las teorías de la comunicación al estudio de la sesión psicoanalítica, le interesó siempre grabar ciertas sesiones y detectar en las diferentes voces de los pacientes, las melodías, armonías, rubattos, contrapuntos, disonancias, que hubiera en ellas[[41]](#footnote-41).

Los descubrimientos de este psicoanalista argentino son fundamentales métodos de observación de los datos que nos proporcionan los pacientes y del efecto que en el paciente producen las interpretaciones del terapeuta. Liberman también se agrupó con los que consideraban al análisis como inductor de transferencia y trabajó en ese sentido.

Este autor se propuso volcar los principios básicos del psicoanálisis (libido, inconsciente, transferencia, fijación) a la teoría de la comunicación, y tomando las áreas de la sintaxis (reglas de la comunicación), semántica (sentido manifiesto y latente de la comunicación) y pragmática (conducta en la transferencia) armó su teoría acerca de los estilos comunicacionales.

Cada estilo puede definirse como un conjunto de operaciones retóricas específicas, derivado de la eficacia de las defensas. En cada paciente, la estructura del preconciente es compleja, ya que a veces un estilo constituye una fachada defensiva frente a otro, o bien existe un estilo dominante y otros subordinados. A continuación se sintetizan las características de los seis estilos básicos, tal como fueron expuestas en un libro escrito por el autor: 1) reflexivo, 2) lírico, 3) épico, 4) narrativo, 5) dramático con suspenso, 6) dramático con impacto estético.

Luego se relacionan estas descripciones con las estructuras clínicas respectivas, descriptas en términos de: 1) esquizoidia- esquizofrenia, 2) depresiones- psicosis melancólicas, 3) perversiones, psicopatías, paranoias, 4) neurosis y caracteropatías obsesivas, 5) neurosis y caracteropatías fóbicas y 6) neurosis y caracteropatías conversivas. En cada paciente se da una combinatoria específica de los estilos recién enumerados.

Este método consiste en tomar como parámetro de comparación las fantasías primordiales y sus transformaciones derivadas por un lado de la defensa y por el otro de la erogeneidad específica con que se tiñen las formaciones sustitutivas. A esta exposición se agrega un intento de distinguir entre la transformación retórica y perturbación estilística, término éste con el cual Liberman distinguía la patología.

Concisamente puede definírsela “como falla en el esfuerzo por hallar una transacción retórica que permita conciliar el triple vasallaje del yo, ante la pulsión, el superyó y la realidad. En tal caso se pierde o bien la posibilidad de expresar al ello, o bien queda desafiada o abolida alguna norma consensual específica”[[42]](#footnote-42).

En concordancia con estos estilos de comunicación del paciente, estarían los estilos o registros en que debería moverse óptimamente el analista en la sesión clínica, para provocar efectos estructurantes en el paciente, que en la nomenclatura de Liberman, sería “favorecer un cambio en el registro o estilo del paciente”.

Para dar un ejemplo, si el paciente está en el registro de “la persona demostrativa” el análisis tendría que manejarse en el de la persona “observadora y no participante”.

**4.3 – La delincuencia de cuello blanco y de guante virtual**

Debemos a Edwin Sutherland la introducción, a principios de los años cuarenta, del término “delincuencia de cuello blanco”,[[43]](#footnote-43) para referirse a aquel tipo de acciones ilegales llevadas a cabo por los miembros más acomodados de la sociedad –delitos de la clase alta-, tales como fraude fiscal, desfalcos, ventas fraudulentas de propiedades, contaminación ilegal del medio ambiente, por oposición a los delincuentes de bajo status socio-económico.

Sutherland señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

En términos generales, las características personales del delincuente de cuello blanco son: alto nivel socio-económico-cultural, meticuloso, detallista, con facilidad en la expresión verbal, capacidad de organización y planeación, manipulador, baja introyección de valores, materialista, falta de empatía, alto control de impulsos, alta tolerancia a la frustración, personalidad con rasgos obsesivo-compulsivos (DSM-IV), necesidad de gratificación (status y reconocimiento), seductor y provocador.

Asimismo, tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete y a las diferentes formas de cometerlo.

Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza, por mala habitación, por carencia de recreación, por baja educación, por poca inteligencia, ni por inestabilidad emocional.

El Sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Permite conocer los diferentes ilícitos que cometen los delincuentes informáticos, como también prever estas acciones; ya que muchos de los delitos son descubiertos casualmente por el desconocimiento de la forma de operar de los sujetos activos.

En el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones o gobiernos, que usan sistemas automatizados de información, generalmente conectados a otros.

En la actualidad en los medios de comunicación se les denomina delitos de guante virtual a los actos que realizan sujetos para delinquir a través de medios digitales.

**4.4 – La personalidad y los estilos comunicacionales**

La personalidad es el término con el que se suele designar lo que de único, de singular, tiene un individuo, las características que lo distinguen de los demás. El pensamiento, la emoción y el comportamiento por sí solos no constituyen la personalidad de un individuo, ésta se oculta precisamente tras esos elementos.

La personalidad, también implica previsibilidad sobre cómo actuará y cómo reaccionará una persona bajo diversas circunstancias.

Las distintas teorías psicológicas recalcan determinados aspectos concretos de la personalidad y discrepan unas de otras sobre como se organiza, se desarrolla y se manifiesta en el comportamiento

Una de las teorías más influyentes es el psicoanálisis, creado por Sigmund Freud, quien sostenía que los procesos del inconsciente dirigen gran parte del comportamiento de las personas.

Allport por su parte, definía a la personalidad como formas relativamente estables, características del individuo, de pensar, experienciar y comportarse.

La personalidad se diferencia del temperamento, ya que este consiste en la herencia biológica recibida y por lo tanto difícil de cambiar o modificar.

Se puede decir que incluye el sustrato neurológico, endocrinológico y bioquímico desde el cual la personalidad comenzará a formarse.

El carácter, por su parte, es un término derivado de una palabra griega que significa grabado y se forma por los hábitos de comportamiento adquiridos durante la vida. Millon piensa que el carácter puede ser considerado como adherencia de la persona a valores y costumbres de la sociedad en que vive.

La personalidad es la conjunción del temperamento y el carácter en una única estructura; representa un patrón profundamente incorporado de rasgos afectivos, emocionales y conductuales manifiestos que persisten por largos períodos y son relativamente resistentes a la extinción.

Podemos citar las siguientes características de la personalidad:

- No tiene una existencia real, se infiere a partir de la conducta de los individuos,

- Es la forma habitual de comportamiento de cada individuo, comprende tanto su conducta manifiesta como su experiencia privada.

- Se desarrolla y se cambia a lo largo de la vida.

- Se produce por la interacción de la herencia genética, el ambiente, el aprendizaje social y las experiencias personales.

- Es individual y social. Cada persona es única e irrepetible.

Las personas desarrollan sus personalidades con aspectos normales y aspectos neuróticos. Esto va a dar lugar a estilos o estructuras de personalidad diferentes con características positivas y negativas.

David Liberman describe los estilos comunicacionales que predominan en cada persona. Los estilos comunicacionales son modos de interacción y estructuras psicopatológicas relacionadas.

Cada área, conformado en su base por el cuadro lógico de Aristóteles, regido por los principios de contrariedad, contradicción e implicancia, tiene un estilo.

Cada punto de fijación, y por consiguiente de regresión en la transferencia corresponde a un tipo o modelo de la comunicación de Ruesh.

Esta clasificación muy sintéticamente sería la siguiente:

Área 1- Esquizoidía. Estilo reflexivo. Observar-sin participar-participar-ser observado.

La persona observadora no participante, corresponde al paciente esquizoide fijado en la etapa oral pasivo de succión.

Cuando este estilo funciona operativamente, posee la capacidad de distanciarse, de observar a distancia sin participar, y tener una visión macroscópica de las cosas.

Se comunican fríamente, sin emociones, despierta en el interlocutor una sensación fría.

Predominan la disociación, idealización y negación como mecanismos de defensa.

Área 2- Ciclotimia. Estilo Lírico. Ser querido - ser perdonado – no ser perdonado – no ser querido.

La persona depresiva, es el melancólico y ciclotímico, fijado en la etapa oral secundaria, activa canibalística.

Cuando funcionan operativamente tienen una visión microscópica, empatía y vínculo con el otro. Sus defensas psíquicas predominantes son la idealización, negación, disociación y las defensas maníacas.

Su discurso suele estar cargado de afecto, amor y odio. Despiertan en el interlocutor emociones calientes: bronca, amor, odio, pero no por seducción.

Área 3- Psicopatía. Estilo épico. Perseguir a los demás – ser justo – ser objeto de injusticias – ser perseguido por los demás.

La persona de acción es el psicópata o el perverso fijado en la etapa anal expulsiva.

A nivel comunicacional utilizan bien la semántica y la sintaxis, pero usan la pragmática para inducir al otro cuando captó su atención. Impacta pero no seduce, capta la voluntad. Su defensa psíquica principal es el control omnipotente.

Lo operativo de este estilo es el paso a la acción y la posibilidad de liderazgo.

Área 4- Obsesiva. Estilo narrativo. Ser ordenado – ser virtuoso – ser vicioso – ser desordenado. La persona lógica, paciente obsesivo, fijado a la etapa anal retentiva. Controla la agresión a través de las defensas. Lo vicioso y desordenado es percibido como agresivo.

En la emisión de mensajes, suelen hablar mucho y despiertan en el interlocutor una sensación de aburrimiento.

Sus defensas predominantes son el control, racionalización, formación reactiva, aislamiento y anulación.

Lo adaptativo de este estilo es que dominan el pensamiento reflexivo y el control de los impulsos.

Área 5- Fobia. Estilo suspenso. Dramatizar – controlar el peligro – no poder controlar el peligro – fracasar en la dramatización.

La persona atemorizada y huidiza es el carácter fóbico, la histeria de angustia con fijación uretral genital.

Utiliza la pragmática para controlar el peligro de la angustia de castración. No dramatiza para seducir, sino para cuidarse del peligro de castración.

Las defensas utilizadas son la evitación, el control, el desplazamiento y la inhibición.

En su forma de comunicarse hay mucho suspenso en su discurso. Puede hablar ordenada y meticulosamente, cuando de repente cambia, desordena y hace virajes, justamente por la evitación.

Lo adaptativo de este estilo es que cuando su ansiedad es operativa moviliza a la acción.

Área 6- Histeria. Estilo poético. Dramatizar – provocar un impacto estético – provocar un impacto de fealdad – fracasar en la dramatización.

La persona demostrativa sería la histeria de conversión, fijada en lo fálico-genital o edípico. Su mecanismo defensivo principal es la represión.

En su discurso dominan muy bien los tres aspectos de la comunicación: la semántica, sintaxis y pragmática, lo que les permite crear un clima de impacto y seducción.

Su conflicto básico pasa por la sexualidad y represión. Lo operativo de este estilo es que integra armoniosamente el pensamiento, las emociones y la conducta.

Algunas características principales de dichas personalidades se resumen a continuación:

**4.4.1 – La personalidad reflexiva**

Son personas agudamente observadoras, austeras con un predominio de lo racional. Son generalmente buenos escuchas y más bien pasivos. Disociados. Su ideal del yo es muy alto, así como su conciencia y su moral. Tienden a manejarse ingenuamente y se mueven con la lógica y por lo general no comprenden aquello que no siga esa lógica. Necesitan estar solos y disfrutan de esa soledad.

Toman distancia y necesitan de ella para funcionar bien. Discriminan lo fundamental de lo accesorio con facilidad, y funcionan bien en las actividades autónomas; no les gustan los horarios fijos ni el control.

Es su necesidad de autoexcluirse emocionalmente constantemente, es él quien excluye al otro, lo único que puede hacer es observarlo sin participar. Tener permanentes sospechas (incógnitas) acerca de las demás personas a quienes observa y estudia omniscientemente como “bichos raros”.

Les cuesta expresar los afectos. Están todo el tiempo pensando y analizando, pero normalmente muestran el final de frase.

Tienen miedo a la agresión, evitan los conflictos pero se mueven en términos de blanco o negro. Se desempeñan muy bien en tareas que deban realizarse individualmente, utilizando la capacidad de abstracción.

Requieren una posición para mirar desde lejos, rechazan la invasión, pero son muy dependientes a pesar de parecer desapegados.

En términos transferenciales dan sensación de no conectarse ni intimar, si bien están pendientes de los gestos del terapeuta.

Son muy autoexigentes y los exámenes internos no se pasan. Funcionan bien en relaciones complementarias con la personalidad histérica, siempre y cuando no sea invadido en su mundo interior.

La estructura esquizoide lleva implícita la dificultad en participar (dar), sumada a una urgencia voraz por observar (tomar, conocer e incorporar). Por eso desde la clínica suelen ser los pacientes más silenciosos y exigentes.

Este estilo posee la capacidad de disociarse, de observar sin participar para percibir totalidades con los detalles distinguibles dentro de dichas totalidades.

**4.4.2 – La personalidad lírica**

Es importante discriminar entre las personas deprimidas y las personalidades depresivas. La depresión es esperable en distintos momentos de la vida, crisis, destetes, duelos y cursa un proceso de elaboración del hecho que produce la depresión. En las personas depresivas hay poca objetividad referida a su autoestima. El autorreproche es permanente con beneficios secundarios de la enfermedad.

Son personas muy rígidas en las normas, con excesivo sentimiento de culpa y autoestima precaria. Necesitan contacto y reaseguramiento. Son poco autónomos. La capacidad de independencia está interferida por la necesidad de conservar la autoestima a costa de los suministros provenientes de objetos de cuya actividad depende. Son sumisos, pero debe tenerse en cuenta que todo sumiso es un agresor en potencia.

Por lo general han sido sobreprotegidos en su crianza, por lo tanto dependen exageradamente de otros; tienen necesidad de seguir siendo sobreprotegidos y a veces reactivamente se transforman en sobreprotectores también ellos.

Presentan un Superyo rígido; estos ideales tan altos pueden conducir a un colapso depresivo. Tienen una ética infantil, regida por la autoestima. Escinden muy marcadamente entre lo bueno y lo malo.

En este tipo de personalidades, si hay componentes maníacos, o hipomanías, el ritmo es el opuesto al depresivo. Llega a hacerse agotador su nivel de actividad. El contacto con los objetos es efímero y superficial, rápidamente se gastan y tienen que ser sustituidos por otros. Son personas omnipotentes, negadoras de la realidad y que tienden a denigrar a los otros para sentirse compensatoriamente triunfantes.

Necesitan conexiones de realimento permanente y el típico humor mantenido a toda costa, da lugar a una forma de relación muy característica, donde juegan en los grupos los roles de animadores.

Presentan la capacidad de acercar la función perceptual al objeto y ver un detalle haciendo abstracción de la totalidad, pero sin confundir la parte con el todo.

**4.4.3 – La personalidad épica**

Las personalidades de acción o épicas, desarrollan su acción impulsiva de una manera veloz, en el sentido de que el lapso entre el pensamiento y la ejecución es generalmente breve y sin planificar. Esto revela una deficiencia en ciertos procesos mentales.

En la persona normal, el antojo o la inclinación a medio formar para hacer algo, es el comienzo de un proceso complejo. En la persona impulsiva su objetivo es la satisfacción de dicha urgencia. No toleran la frustración. Tienen reglas propias y dividen para imperar. No toleran los límites, ni los tienen, su mayor éxito es que no sepan como son. Toman y abandonan episódicamente las parejas, los trabajos y cualquier cosa estable. Su característica fundamental es el aburrimiento y el tedio.

Su trastorno de la capacidad de pensar con símbolos verbales acerca de las cosas que necesitan, da lugar a la manera típica de reaccionar ante una frustración y una forma particular de experimentar angustia, siente tensión y depresión y sufren tedio o hastío.

Experimentan alivio con una actuación psicopática. En ellos aparece la necesidad de hacer algo, pero sin saber qué, acompañado todo esto de un malestar que les provoca tensión, malhumor e irritabilidad a todo tipo de estímulos.

Las personas con estas características poseen una modalidad de comportamiento específica y muchas veces no presentan síntomas manifiestos. En su comportamiento no muestran indicios que indiquen una forma asocial y solamente su conducta pasada futura mostrará la más destructiva de todas las formas conocidas.

No tienen sentimientos de culpa y su aparente temor es más bien paranoide. Producen fascinación en los oyentes y una suerte de impacto que hace que en poco tiempo se sienta que se los conoce de toda la vida.

Poseen una ética propia y tratan a los demás como su superyo los trata a ellos.

Las personalidades psicopáticas buscan consumar con un tercero un acto de venganza -que ellos consideran justiciero- por las injurias narcisísticas sufridas en el curso de la vida, en especial en la temprana infancia. En general en la niñez, los futuros psicópatas no han sido reconocidos como personas autónomas sino como meros objetos de gratificación de los padres.

Utilizan la inoculación, con mensajes que constituyen una orden en el receptor (actuación). De esa manera el emisor procura apoderarse de la voluntad del receptor para sacar un beneficio en detrimento de éste.

Tienen pensamiento concreto y actitudes en última instancia autodestructivas.

Necesitan tener hijos, toman a la mujer como mamá y son comunes las combinaciones con personas depresivas con exceso de sentimiento de culpa.

Poseen la capacidad de captar los deseos propios y llevarlos a la acción en tanto existe la posibilidad de satisfacer dicha necesidad, y para ello tomar una decisión luego de haber calibrado el equilibrio entre necesidad y posibilidad.

**4.4.4 – La personalidad narrativa**

Tienen un modo formal de relacionarse, suelen estar cuidadosamente arreglados, sin descuidar los detalles. Esto no está al servicio del impacto estético, sino del orden, la limpieza y la prolijidad. Son personas caracterizadas por el orden y el control del mundo externo. Tienen temor al cambio. Buena relación con la realidad siempre que se presente ordenada.

Previene situaciones y se fuga en la realidad formal. Tiene buen registro de las representaciones mentales.

Son personas controladas, con un tipo de pensamiento rígido y estructurado y con poca capacidad de adaptación a las distintas situaciones a lo largo de su vida.

No hay mucho espacio para el sentir o el placer en su vida. Están más preocupados por el cumplimiento del “deber”, en hacer las cosas correctamente.

Son personas de código moral estricto, tenaces y cumplidoras.

Así como son ahorrativos en la expresión de sus afectos, son también económicos con el dinero. Dudan permanentemente e intentan salir de la duda con un tipo de pensamiento dogmático. Esta característica los lleva a postergar la acción.

Esto que se presenta como una modalidad ordenada, pulcra y de corrección tiene su contrapartida en fuertes impulsos que necesitan controlar. Surgen como actos o dichos, opuesto a toda esa ceremonialidad descripta, pues la ambivalencia (amor-odio), es una característica que los acompaña.

En cuanto a las funciones yoicas, la atención está orientada hacia los detalles, tanto de sí mismos como del otro. La memoria tiende a recordar hechos concretos más que lo afectivo. Y a nivel de la percepción, está más asociada a los detalles que al conjunto. Como si solo pudieran ver el árbol y no el bosque.

Tienden a disociar la carga afectiva de los recuerdos, por lo que en la relación transferencial, aburren. Al revés de la personalidad histérica, que cuenta emocionalmente los hechos, el obsesivo relata los temas con el mismo tono y con todos los detalles. Sus relaciones afectivas y eróticas son formales, son rígidos y les cuesta ser espontáneos. La agresión se les filtra en las defensas, sorprendiéndolos.

La utilidad es siempre rescatada con el orden y la previsión. La independencia está interferida por la rigidez de las normas y por la sustitución del valor concedido a la palabra en desmedro de los hechos. La obsesividad gira en torno a la duda y el ritual.

Utilizan los rasgos de carácter en actividades donde el orden sea de primordial importancia, se trate de oficinas, archivos, secretarias, y actividades similares.

Su motivo de consulta clínica suele referirse a su angustia por los conflictos que le produce su modalidad obsesiva -excesos de tiempo en las tareas, no discriminación de lo fundamental y lo accesorio, pérdida de control y ansiedad.

Se defienden con el aislamiento, la anulación y las formaciones reactivas.

Posee la capacidad de adaptarse a las circunstancias, al tipo de vínculo, ya sea en el sentido vertical (abuelos, padres, hijos), o en el sentido horizontal (grados de intimidad); la capacidad de utilizar el pensamiento como acción de ensayo, y también la capacidad para estar solo.

**4.4.5 – La personalidad dramática con suspenso**

La actitud de temor y cuidado es el rasgo más sobresaliente de este tipo de personas. Se muestran solícitos y respetuosos, pareciera que están permanentemente pidiendo permiso o perdón. Esto no se debe como en la modalidad lógica a una formalidad, sino a la sensación de que un peligro acecha y encuentran de este modo la forma de controlarlo.

Mantienen una relación infantilizada con el otro. El control que intentan ejercer, mostrándose alertas, está al servicio de sentirse a salvo.

Suelen hablar en voz baja y en forma lenta. Son de pocas palabras, como si las estuvieran midiendo.

Necesitan mantener con el otro una “distancia óptima”, ni demasiado cerca como para vivirlo como un peligro, ni demasiado lejos como para sentirse no tenidos en cuenta. Se percibe una cierta sensación ansiosa en ellos.

Tienen mucha necesidad de afecto pero al mismo tiempo, necesidad de moverse sin que lo encierren. Por lo general buscan un objeto acompañante y esta dependencia es la que los vuelve evitativos. Presentan problemas en todo lo relacionado con la angustia. Su vida pasa por lo que le produce o no angustia.

Sus fobias van de la claustrofobia a la agorafobia, de la castración al abandono. El fóbico acorralado se pone paranoico. En su vida diaria son independientes y funcionan en tareas autónomas y con movilidad.

Esta movilidad les permite ser muy creativos y no se adaptan a las rutinas. Son personas con mucha independencia, que encubre su dificultad para establecer vínculos, por su temor a quedar encerrados y sin aire. Así, su agresión se convierte en ansiedad e impulso a la fuga. En la sexualidad pueden presentar eyaculación precoz y recursos infinitos para huir.

Desde lo clínico su motivo de consulta se relaciona a la angustia, ataques de pánico, fobias específicas. Transferencialmente producen ternura y sensación de protección. Sus mecanismos de defensa habituales son la evitación, el desplazamiento –sobre un objeto que se controla- y la contrafobia -huida hacia delante.

En cuanto a las funciones yoicas, la atención es generalizada, abarca todo el campo. La memoria suele recordar sobre todo aquellas situaciones que le resultaron angustiosas. Tienen un tipo de percepción general inmediata, que de entrada la instrumentan como modo de reasegurarse.

Poseen la capacidad de tener un monto de ansiedad útil preparatoria para llevar a cabo una acción, una vez establecido el vínculo, tomada la decisión y observadas las circunstancias.

**4.4.6 – La personalidad dramática con impacto estético**

Es una personalidad que muestra, exterioriza. Se expresa con una gran riqueza mímica y verbal. En general son personas muy atractivas y seductoras, con tendencia a la dramatización. Su modo de presentarse no pasa inadvertido. Poseen una gran plasticidad y teatralidad. Parecen vivir todo con mucha intensidad, lo que les permite producir en el otro un fuerte “impacto estético”.

Su lenguaje es pleno de adjetivos, dan pocos datos concretos. Su lenguaje es rico en metáforas. Ejemplo: “me duele el corazón” o “me clavó un puñal” para hablar de un dolor amoroso. Tienen gran capacidad simbólica.

Hablan de sus emociones y sentimientos fácilmente. Su particular facilidad de expresión se debe a que las emociones, el lenguaje y el gesto están perfectamente coordinados. Tienen por lo tanto muy buena capacidad para expresarse en las tres áreas del comportamiento: mente, cuerpo y mundo externo.

El cuerpo es la zona de manifestación por excelencia y no pasa inadvertido, no sólo a nivel de sus dolencias sino en su modo de presentación: adornos, vestimenta, maquillaje, etc.

Son personas que captan rápidamente el interés del otro y tratan de adaptarse a lo que suponen se espera de ellos. En las relaciones les cuesta hacer verdaderos contactos.

Tienden a ser centros de atención y no les molestan las situaciones de exposición, si bien en ese lucirse, suelen depender enormemente de la mirada de otros. Suelen presentar problemas en la sexualidad, frigidez o impotencia.

Su necesidad de llamar la atención y su afán de hacerse notar está al servicio de seducir y estar ubicados en el “centro de la escena”. Necesitan ser estimados. Tienen por lo tanto un beneficio secundario, ya que muchas veces logran llamar la atención de su familia y su entorno (por ejemplo, con alguna dolencia física).

En la práctica clínica suelen consultar por problemas en el cuerpo, conversiones que no son explicables desde el punto de vista médico, donde el cuerpo es un área de expresión de conflictos y la idea de simulación; y por dificultades de pareja.

Transferencialmente suelen producir rechazo al parecer dominante y autosuficiente, pero en realidad son muy dependientes de la opinión de los demás e inseguras en su base. Tienden a defenderse con impactos, haciendo conversiones o con seducción. La defensa típica es la represión. Reprimir es no querer saber de una serie de experiencias que el individuo tiene dentro de sí, en tanto su recuerdo suscita angustia.

En relación a las funciones yoicas, presentan la atención dispersa. Son personas que pueden percibir distintos estímulos simultáneamente. Su memoria está más asociada a los afectos que a los hechos. Si cuentan alguna situación particular es probable que incluyan más lo que sintieron que los datos objetivos del momento. En cuanto a su percepción, tiende más a lo global que a los detalles.

Poseen la capacidad de enviar un mensaje en el cual la acción, la idea y la expresión del afecto se combinan adecuadamente.

En síntesis, los estilos de personalidad clasificados por Liberman se incluyen en el siguiente cuadro, visualización que ha facilitado la tarea de análisis sobre los delincuentes informáticos, que en general, responden a las pautas determinadas en las columnas grisadas del cuadro mencionado.

Cuadro III - Clasificación de estilos de personalidades según Liberman[[44]](#footnote-44)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Esquizoide** | **Ciclotimia** | **Psicopatías** | **Obsesivo** | **Fóbico** | **Histérico** |
| Paciente reflexivo que busca incógnitas sin crear suspenso (Esquizoide) | Paciente lírico (Depresivo) | Paciente épico  (Persona de acción) | Paciente narrativo.  (Persona lógica) | Paciente que dramatiza, busca incógnitas y crea suspenso.  (Persona atemorizada y huidiza) | Paciente que dramatiza y crea impacto estético.  (Persona demostrativa) |

**4.5 – Sujetos detrás de los delitos informáticos**

Según Palazzi, en “Delitos Informáticos”, considera que es un mito que el delincuente informático deba forzosamente poseer conocimientos técnicos profundos. A su juicio la computación se halla tan extendida actualmente, que “cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa, puede realizar un delito informático. Es inducido a delinquir por la oportunidad que se le presenta frente al uso diario del ordenador y la impunidad que éste le brinda”.[[45]](#footnote-45)

Este autor, a partir de la experiencia comparada e incluso la nacional, clasifica los perfiles en los siguientes grupos:

|  |  |
| --- | --- |
| **Cuadro I – Clasificación de delitos y perfiles** | |
| ***Clase de delito*** | ***Sujetos*** |
| Delitos patrimoniales contra bancos y entidades financieras | Empleados, en especial cajeros o personal del área de sistemas, ex empleados, terceros en connivencia. |
| Delitos de acceso ilegítimo o delito de daños menores. | Hackers, phreakers, usuarios descontentos. |
| Daño o sabotaje informático. | Empleados de la empresa, o espías profesionales e industriales. |
| Violaciones a la privacidad, tratamiento ilícito de datos personales. | Investigadores privados, empresas de marketing, agencias de informes crediticios y de solvencia patrimonial. |
| Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos. | Piratas informáticos, o también usuarios (“la copia amigable”), empresas que realizan competencia “parasitaria”. |

Fuente: Cuadro de Palazzi. Op. cit.

Para este autor, el delito informático es más difícil de investigar que el delito tradicional porque es novedoso, escapa a los cánones tradicionales, los cuerpos policiales y tribunalicios no están preparados para investigar y detectar estas técnicas novedosas y el propio delito suele no dejar rastros. En el ambiente digital no quedan huellas visibles a simple vista, y si éstas existen es muy difícil imputarlas a una determinada persona.

Existiría además, una disociación espacial y temporal en la realización de estas actividades. Estas dificultades hacen que sólo la confesión del autor permita su condena. En Estados Unidos es un claro ejemplo el caso Morris. Si Robert Morris no hubiera confesado ser el autor del programa que infectó más de 6.000 ordenadores, no podría haber sido condenado, pues no existían pruebas materiales que lo unían a la programación del virus. (Ver Caso Nº 7)

**4.6 – Algunos estudios sobre las características de personalidad**

Las personas que cometen los delitos informáticos son aquéllas que poseen ciertas características que no presentan el denominador común de los delincuentes; habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la realización de este tipo de delitos.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la Prevención y Control de Delitos Informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. En relación a las características personales de aquellos que cometen delitos en alta tecnología, debe tenerse presente generalmente lo siguiente:

- En general son personas que no poseen antecedentes delictivos.

- La mayoría son de sexo masculino.

- Actúan en forma individual.

- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación "hackers".

- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismos.

- También hay técnicos no universitarios, autodidactas, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

- En el caso de los "hackers", ellos realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovecha la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).

- Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia los han catalogado como "delitos de cuello blanco", esto se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.[[46]](#footnote-46)

En 1997, el Departamento de Defensa de los Estados Unidos auspició un proyecto que fue conducido por Eric D. Shaw, Jerrold M. Post y Keven G. Ruby[[47]](#footnote-47). En este estudio criminológico se llegó a la conclusión de que si bien los sujetos que habían cometido delitos informáticos no siguen un patrón específico, sí existe una serie de rasgos compartidos por muchos de ellos. De este modo, Shaw, Post y Ruby establecieron las siguientes características psicológicas:

*Introversión:* persistió que los introvertidos se sienten más cómodos en su propio mundo mental que en el mundo social, que es más emocional e impredecible. Son más sensibles que los extrovertidos a presiones externas y tienden a poseer habilidades sociales menos sofisticadas.

*Frustraciones:* muchos de los sujetos tenían un historial de problemas familiares significativos, dificultades en la escuela, en el trabajo y diversas frustraciones sociales, que les dejaron con actitudes negativas hacia la autoridad.

Estos hallazgos coinciden con la investigación del profesor R. Caldwell, científico en computación, que en estudios conducidos separadamente en 1990 y 1993, halló altos niveles de decepción y conflicto entre un grupo de estudiantes de ciencias de la computación, quienes manifestaron que preferían la estructura y el carácter predecible de las computadoras, a las variaciones en las relaciones personales.

*Dependencia de la computadora*: para muchos de estos sujetos, la actividad ‘on line’ o en línea, interfería o reemplazaba sus interacciones profesionales o sociales directas. Según Shaw, Post y Ruby, estos individuos manifestaban como intereses principales explorar las redes informáticas, violar códigos de seguridad, penetrar en sistemas y desafiar y competir audazmente con profesionales de seguridad. Además, pensaban que los dependientes de computadoras tendían a estar profundamente involucrados en relaciones en línea, al extremo de preferir su personalidad 'on line' a su personalidad en el mundo real con sus propias relaciones.

*Flexibilidad ética*: los sujetos informaron que no veían sus trasgresiones como carentes de ética; algunos incluso las justificaron debido a las circunstancias. En 1995, S. Harrington realizó una investigación sobre este tema “Límites éticos dentro de la cultura de la información”. Anticipándose a las conclusiones de Shaw, Post y Ruby, los hallazgos de Harrington indicaron que aproximadamente el 7% de los profesionales de la computación no se oponen a las penetraciones, espionaje o sabotaje. En su lógica, atacar un recurso electrónico es un juego aceptable, si es que no ha sido dotado de un robusto sistema de seguridad.

Otros fenómenos sociales han sido citados como contribuyentes a dicha flexibilidad ética, incluyendo la falta de entrenamiento en ética informática, la carencia de políticas y regulaciones específicas sobre privacidad y seguridad, la ausencia de sanciones legales por los abusos y la falta de interacción cara a cara en el ciberespacio.

*Reducida lealtad*: según Shaw, Post y Ruby, estas personas parecieron identificarse más estrechamente con su profesión o especialidad en las computadoras, que con su supervisor. Esta conclusión recuerda un estudio sobre fraude con computadoras, efectuado por el Departamento de Salud y Servicios Humanos de los EEUU en 1986, el cual encontró que los programadores que cometieron fraude se sentían más leales a su profesión que a su supervisor o jefe.

*'Entitlement' o sentido de tener derecho*: es la sensación de que uno es especial y que merece el respectivo reconocimiento, privilegio o excepciones. Fue una característica básica en muchos de los atacantes y este rasgo fue frecuentemente reforzado por el supervisor. Al unirse con una previa indignación contra las figuras que representan autoridad, como sucedía con frecuencia, esta sensación de merecimiento aumentaba el deseo por la revancha, como reacción por los desaires y menosprecios.

*Falta de empatía:* los investigadores observaron en los empleados un desinterés por el impacto de sus acciones sobre otros o su incapacidad para apreciar este impacto. De igual modo, muchos de los individuos en este estudio carecían de empatía. Esta característica se magnifica por la naturaleza del ciberespacio, en donde el efecto de los hechos no se percibe por la falta de consecuencias inmediatas.

Los autores de este estudio explican que una característica de los delincuentes informáticos es que tratan de minimizar o malinterpretar las consecuencias de sus actividades, justificando que con su comportamiento están llevando a cabo un servicio realmente útil a la sociedad.

Estos investigadores han decidido calificarlo como Síndrome de Robin Hood, por el nombre del personaje del cuento quien robaba a ricos para darles a los pobres lo que creía que les correspondía. En este caso, ellos consideran que la información es algo que no debe ser sólo de algunos – ricos - sino que debería estar al alcance de todos.

También tratan de deshumanizar y culpar los sitios o víctimas que atacan. Post señala que los mismos piratas informáticos comparten un sentido de "flexibilidad ética"; esto quiere decir que debido a que el contacto humano es minimizado sobre la computadora, piratear se hace de la misma manera que un juego donde las consecuencias serias pueden ser omitidas fácilmente. Pero es cuidadoso al mencionar que no todos los hackers son criminales.

Según ellos es una población que se refugia en computadoras debido a sus problemas para mantener las relaciones con el mundo real, causando millones de dólares en daños, lo que les da unos aires de grandeza verdaderos.

**4.7 – Motivaciones:**

Según Barón, el término motivación se refiere a los procesos internos que sirven para activar, guiar y mantener la conducta a lo largo del tiempo[[48]](#footnote-48).

Algunos autores han clasificado la motivación en:

*Intrínseca:* no persigue otro premio que nuestra propia satisfacción. Este tipo de motivación está fuertemente relacionada con las necesidades psicológicas.

Los sujetos con motivación intrínseca no persiguen explícitamente el dinero.

*Extrínseca:* aquella que se guía en función de los resultados de nuestra acción, ya sean estos positivos o negativos. Se basa en el viejo sistema de premios y castigos. Las personas que pretendan atacar una organización con una motivación extrínseca buscarán simplemente el premio, o sea, dinero o bienes cambiables por dinero.

La motivación en el ataque o en amenazas informáticas supone también un aspecto clave en la diferenciación de perfiles, ya que hackers, crackers, phreakers y viruckers, teniendo parecida capacidad y disponiendo de las mismas oportunidades, terminan realizando ataques distintos.

Algunos estudios realizados sugieren que los factores que afectan la motivación de los sujetos denominados *hackers* o piratas informáticos hacia actividades ilegales no se encuentran definidos claramente. Es conocido, por ejemplo, que pocos delincuentes informáticos son motivados por beneficios económicos. La mayoría de las actividades hacker son de una naturaleza donde el dinero es raramente involucrado.

En general los estudios consultados coinciden en que las características que motivan a estos sujetos son las siguientes:

*Curiosidad:* muchos piratas informáticos han dicho que son sólo "curiosos" por las computadoras y las redes telefónicas y cómo funcionan.

*Espiar*: a algún amigo/a o miembro de la familia, un colega de trabajo o empleado, o a una empresa rival. Involucra generalmente la observación de personas individuales en sus actividades en Internet o a sus datos personales, durante cierto período de tiempo sin que ellos noten esta vigilancia.

*Prestigio*: credibilidad o prestigio social dentro de la comunidad hacker, pueden elegir una meta prominente, que adquirirá la cobertura a la perfección en los medios de comunicación más importantes como los periódicos o la televisión.

*Desafío intelectual*: éstas son dos palabras que aparecen una y otra vez cuando los delincuentes informáticos condenados son entrevistados. Muchos piratas informáticos “*black hat*” (sombrero negro) sólo gustan de la emoción de romper un servidor, y pudieron haber estado trabajando para “crackear” o romperlo por meses.

*Anarquía:* aunque menos común que los factores anteriores, algunos piratas informáticos tienen ideas anti-globalización combinadas con un odio por la naturaleza corporativa de muchos sitios de comercio electrónico. Esperan hacer caer estos sistemas financieros para reclamar la Internet para sí.

*Dinero*: La mayoría de los hackers no son motivados por beneficios financieros, si participan en el fraude de tarjetas de crédito es para comprar nombres de dominios [[49]](#footnote-49)o espacios Web[[50]](#footnote-50).

Tal como se ha podido apreciar, los estudios psicológicos de los delincuentes que utilizan medios informáticos son variados y han sido estudiados desde distintos ángulos, pero coinciden en la mayor parte en sus observaciones finales, por lo tanto son significativos para propiciar el resto de esta investigación.

**Capítulo V**

**Materiales, métodos y procedimientos**

**5.1 – Objetivos e hipótesis de trabajo**

El objetivo general de la investigación se centró en la realización de una aproximación al estudio del fenómeno de los delitos informáticos y de los sujetos que se encuentran detrás de ellos.

Por su parte, los objetivos específicos han consistido en conocer las características de los delitos informáticos; investigar el impacto de estas conductas en la vida social y tecnológica de Occidente durante los últimos cuarenta años y presentar una aproximación a los perfiles de personalidad característicos de los sujetos que realizaron delitos informáticos.

Para llegar a la formulación de una hipótesis de trabajo se plantearon los siguientes interrogantes:

¿Qué son los delitos informáticos? Cada delito informático presenta diferentes características y por eso los rasgos de personalidad de los autores deberían ser diferentes en cada tipo de delito, ¿o son parecidos?, ¿Cómo son?

¿Cómo son las personas que los realizan?, ¿Cuáles son sus principales motivaciones?, ¿Cómo son considerados estos delitos por el Derecho en otros países y en Argentina? ¿Cuáles son las penas en el caso de estar tipificados como delitos?

“Si analizo un conjunto de casos individuales sobre delitos informáticos realizados en el pasado, se podría vislumbrar un patrón de conducta que permita determinar cierto perfil psicológico de personalidad, conducta y de mecanismos delictivos en cada caso. Dichos perfiles podría servir para conocer y prevenir futuros ilícitos mediante el uso de redes y computadoras”.

**5.2 - Metodología de la investigación**

**5.2.1 – Tipo de estudio y diseño**

En este trabajo de investigación nos encontramos con varios problemas a la hora de encuadrarlo dentro de los parámetros de la metodología científica.

En principio nos hemos decidido por considerar que trabajamos en un estudio que se orienta hacia lo cualitativo bajo un diseño no experimental, para lo cual apelamos a las siguientes consideraciones.

A partir del estudio de metodólogos como León y Montero, en lo específico de la ciencia psicológica, o Hernández Sampieri y otros desde la perspectiva de la investigación de las ciencias sociales, se observó que los perfiles de nuestro trabajo no encajaban con la misma claridad con la cual pudimos señalar y definir el campo de la investigación: el ciberespacio y la concepción virtual del mundo de los delincuentes informáticos.

Desde el punto de vista de León y Montero, la perspectiva descriptiva –que creíamos en un primer momento era el método apropiado- no encajaba porque para ello requería de instrumentos como la encuesta y la muestra multitudinaria. Tampoco desde el punto de vista de Hernández Sampieri el trabajo podía incluirse en su concepción descriptiva, porque también se apoyaba en la cantidad y relación directa con los objetos de estudio. Ambas posturas dentro del marco no experimental.

Desde luego que pensamos que podía tratarse del método del estudio de casos, ex post facto, pero tampoco soportaba al trabajo de investigación porque los elementos reunidos no permitían una articulación clara, que nos permitiera analizar los datos en profundidad y mucho menos concluir.

El universo elegido: el ciberespacio y la muestra tomada de él: los delincuentes informáticos presentaban un problema de base. La información publicada en soporte papel sobre ellos es mínima o inexistente; la mayor parte se encuentra inserta en la red Internet, y desde luego, que sólo podían tenerse en cuenta aquellos datos que se encontraban alojados en páginas creíbles.

La otra dificultad, la presentaba la diferente forma de presentar los casos por parte de los organismos que controlan a la delincuencia informática: todos son similares, pero sin un método efectivo que uniformara la información. Había que elaborarla.

Para ello volvimos a la búsqueda de un método de la ciencia psicológica que nos aproximara a nuestro tipo de estudio, sin descartar a los teóricos enunciados, y nos pareció adecuado el planteado por el profesor Marcos Ruiz Soler, de la Universidad de Málaga, quien introduce en su "Metodología de la investigación en las ciencias del comportamiento" (2000), los diseños observacionales, que desplazan lo descriptivo al objetivo de investigación, hace énfasis en el marco realista –en el sentido que este trabajo de investigación intenta ser un cable a tierra del delito informático, que aparece como virtual, pero es real-; frente a este fenómeno el control de las variables es aleatorio, por lo tanto se emparenta con los diseños no experimentales de León y Montero o Hernández Sampieri, puesto que no se tiene control sobre ellas, pero sí se advierte que es posible describir el fenómeno con pocas muestras, pero éstas son significativas por las lecturas que se pueden hacer desde la perspectiva de la metodología de la ciencia psicológica.

Es posible que la variable más controvertida en esta investigación sea el hecho que el trabajo de reconstrucción de las personalidades de los delincuentes informáticos sea a partir de la transformación de datos en documentos analizables, pues en Argentina no se cuenta –y en Mendoza son inexistentes- con muchos casos de delincuentes informáticos detenidos, por lo tanto la relación directa con hechos concretos, tangibles no se pudieron concretar.

Como instrumento para reconstruir –o construir- la personalidad de los delincuentes informáticos, nos basamos en uno propio de la sociología, la historia de vida. La historia de vida –así como la autobiografía- se inscribe dentro de la metodología cualitativa utilizada en las ciencias sociales. La importancia adquirida por este método merece analizarse. Para ello consultamos el artículo respectivo incluido en el Diccionario de Sociología.

El principio epistemológico que sienta Rickert cuando establece la distinción entre Ciencias Naturales y Ciencias de la Cultura, al señalar que estas son ciencias particularizantes, puede contribuir a entender la importancia de la consideración de la "conexión histórica de sentidos" –como lo denominara Dilthey- relativa a ese complejo mundo de relaciones que inciden sobre el fenómeno humano (es decir, cultural) que se quiere conocer (personajes, acontecimientos, pueblo, época, comunidad, etc.).

F. Ferrarotti habla, en este sentido, de "intencionalidad nomotética" e "intencionalidad ideográfica". Todo fenómeno histórico es tal porque se da en un tiempo y en un espacio dado, y en cuanto tal es irrepetible y único, como es la "vida". Es por eso que el historicismo destaque, en la consideración de cada fenómeno histórico-social, elementos como los que se detallan a continuación:

a) la conexión estructural de cada elemento de la vida histórica;

b) la conciencia de la "totalidad de la vida";

c) el correlato o correspondencia hombre-mundo como unidad real y de comprensión;

d) la toma de posición de la conciencia del hombre frente al mundo, concebido ése como "millieu" histórico-cultural.

Dilthey sostenía que el individuo es el elemento sobre el cual sociedad e historia se construían. Para C. Javeau el "individuo" de Dilthey y el "hombre-medio" de Quételet hacen devenir los modelos concurrentes de las construcciones paradigmáticas propias de las Geisteswissenshafen, principalmente a la Sociología. Así Javeau habla de Weber y Simmel en tanto "epígonos" de Dilthey.

Es precisamente Dilthey quien pone el acento, en la primera etapa de su pensamiento, en el conocimiento de la vida como "vivida", es decir, como vivencia; de allí que privilegiara la introspección y promoviera una Psicología descriptiva y comprensiva. Con el tiempo, va corriendo el acento hacia la hermenéutica de la vida histórica. Por eso la importancia que atribuye al conocimiento de los materiales de los archivos, de las correspondencia, de las autobiografías, de los relatos de viajes y de las biografías. Estas últimas nos dan, precisamente, el "Geist" o espíritu de la época; él mismo lo intentó en sus biografías de Hegel y Scheleirmacher.

Dilthey percibió algunos decenios antes lo que Thomas y Znaniecki formularían en la década de los años veinte, a través de sus estudios sociales de la influencia de los valores culturales sobre los individuos colocados frente a una situación de cambio; en dichos estudios se destacan, como método sociológico, la correspondencia y las historias de vida de los campesinos polacos que emigraban a los Estados Unidos de América.

No hay duda que la pretensión de Dilthey fue mucho más allá de lo que se propusieron los autores que estudiaron el tema polaco. Esta distancia que media entre el intento por elaborar una teoría inclusiva que funde la legitimidad de las Ciencias del Espíritu y las pretensiones de una teoría de alcance medio.

En la relación del pensamiento historicista alemán y el método autobiográfico, hay que señalar algo que hace a la historia del problema. Charlotte Bühler y Eduard Spranger, de gran influencia en los comienzos de la Psicología de la Personalidad, fueron discípulos de Dilthey, e introducen en la Psicología el uso del método autobiográfico como procedimiento para una comprensión total de la vida.

De modo que la historia personal emerge como método heurístico. Ya J. B. Vico, en 1731, había descrito el carácter sociológico del "singular". Historia de vida que interesa no sólo cuando se trata del "gran personaje", sino también en el común de las gentes, cualquiera sea el status de éstas.

Es historia –en cualquiera de los casos- de un proyecto único e irrepetible, singular. Aun las formas más agudas de masificación se dan desde la propia individualidad: el sujeto elige "no elegirse" o, al menos, no lucha con convicción contra condicionamientos de variado signo que oprimen su singularidad y libertad.

La historia de vida es individual pero por ser tal –en tanto correspondiente a un sujeto socializado en un tiempo sociocultural propio- es historia de lo social-global, en tanto internalizado a través de sucesivas mediatizaciones: familia, escuela, grupos de pertenencia y referencia, etc. En cierta forma, la historia de vida es a lo sociocultural lo que una célula es al organismo que integra: es individual, tiene entidad y vida propias, pero responde o tiende a explicar el "todo" al que pertenece. La historia de vida aparece como consecuencia necesaria de la revalorización del individuo como actor social. Actor que, más allá de sus condicionantes socioculturales y témporo-espaciales tiene características eminentemente propias; que son conjugadas y "actuadas" de diversas maneras: libertad, intencionalidad, sociabilidad, simbolicidad, eticidad, religiosidad, raigalidad.

La historia de vida es el más difícil medio, pero uno de los más ricos en la investigación porque ahonda en la peculiaridad del "singular" para recomponer y comprender mejor el todo social-global en tanto conformado por el cruce y juego de significaciones y sentidos. El hombre aparece, así, como una "reapropiación singular y simbólica del universo social e histórico" (Javeau, Deltenre).

Ferrarotti descubre en la contextualización del método biográfico, de las historias de vida, la singular existencia histórica, entendida como Dasein, en la unidad permanente del ser-en-el-mundo; más allá de la ilegitimidad de la conclusión que este autor saca cuando, a continuación, afirma que en este ámbito el mismo investigador no sólo resulta externo al estudio sino que se le reconoce su activa participación en la dialéctica investigador-investigado.

Se trata de descubrir lo extraordinario que tiene lo ordinario. Pero este descubrimiento, para darse, necesita no sólo de prerrequisitos gnoseológico sino también éticos: el respeto al otro, el reconocimiento de la alteridad. En la atenta escucha del "otro", el objeto de estudio científico es reconocido también como sujeto. Se está así en presencia de un diálogo de dos interioridades; ambas buscan el autoconocimiento –en término de F. Ferrarotti, la resolución de la "ecuación personal"-, de modo de estar en mejores condiciones de vincular el sistema de la personalidad con los sistemas social y cultural. Esta "vuelta a la interioridad" deviene al mismo tiempo resolución de la "ecuación" socio-histórica.

El método representado por la historia de vida revaloriza la interacción como medio para investigar. El silencio del que escucha es tan activo como la palabra del testimonio.

Asimismo, este método cualitativo representa el tiempo existencial, imbricado –aunque no necesariamente sincronizado- con el tiempo histórico e institucional. Lo cotidiano no es más que el tiempo existencial en un contexto espacio-socio-cultural determinado. Contexto que obra como "paisaje" del texto narrado y, al mismo tiempo, como freno al psicologismo y a lo que Ferrarotti denomina "desviaciones paraliterarias": es necesario un marco familiar, local, comunitario, social y ambiental en general donde insertar –y así mejor comprender- la historia de vida. El contexto obra como "control" no sólo del investigador sino también del investigado.

La sociedad es el producto de perpetuas interacciones entre los individuos y las estructuras, dentro de una temporalidad que confiere a los primeros sus destinos y a las segundas sus historias. Irreductibilidad, pues, del individuo, ya que "si se muere siempre solo, entonces se vive también siempre solo, aun en la más estrecha de las solidaridades." [[51]](#footnote-51)

**5.2.2 - Definición del grupo investigado. Selección de la muestra.**

En la actualidad existen muchas clasificaciones para los navegantes del ciberespacio, de acuerdo con el uso que le dan a su ordenador. En este trabajo de tesis se han tomado sólo aquellas clasificaciones que tengan interés para la psicología, en cuanto puedan configurar una aproximación al perfil de personalidad de estos sujetos que realizaron delitos informáticos, los que son conocidos como hackers, crackers, phreakers y virucker.

Estas cuatro tipologías tienen en común que presentan conductas que van dirigidas a causar alteraciones o daños lógicos en los sistemas informáticos.

Es interesante abordar este tema, ya que se considera que se trata de una actividad que tiene como fin el enfermar a un sistema, agrediendo su normal funcionamiento y evolución en lo virtual del ciberespacio. Pero dentro de los delitos informáticos, son amplios y diversos los modos de agredir el orden, son diversos los motivos e intereses de los múltiples usuarios del ciberespacio, y dentro de esto se ha tratado de clasificar y explicar los diferentes modos de agredir a un sistema, para obtener una ganancia para un fin propio, o para otros; como lo que algunos autores han denominado “síndrome de Robin Hood”.

A comienzos de los '90, Internet era todavía un fenómeno lejano, al que pocos tenían acceso, pero la información restringida y confidencial atrajo a los primeros criminales informáticos.

En aquel tiempo eran catalogados como:

-Sombrero Negro: calificados como terroristas y mercenarios, usaban sus conocimientos para acceder a bases de datos que luego vendían.

-Sombrero Gris: este tipo de piratas se dedicaba a demostrar cuanto sabía y cual era su capacidad para vulnerar sistemas. Su acción nunca fue con la intención de causar daño.

-Sombrero Blanco: detectaban errores y fallas en los sistemas de seguridad y advertían como remediar el problema.

Con Internet el pirateo se simplificó porque los programas fueron puestos a disposición del público en la misma red. Desde entonces, la distinción se hace por los grados de conocimiento y la esfera de su actuar. Así nos encontramos con los Hackers, los Crackers, los Phreakers, y los Virucker; quienes son los grupos originarios de los que se subdividen otros tantos. A continuación distinguiremos cada uno de ellos.

En el Capítulo II se explicó el origen del término y la cultura hacker, algunas características generales de la psicología hacker se describen a continuación:

**Hacker**

La palabra hacker se originó en 1959, con el surgimiento de programadores talentosos que desarrollaron programas que podían eliminar a otros dentro de un mismo sistema operativo.

Se comenzaron a llamar hackers por la identificación con personajes de principios de siglo que nada tenían que ver con las computadoras, pero que brillaban por su excesiva laboriosidad. Estos trabajadores eran los inmigrantes encargados de bajar las maletas en los puertos de Nueva York y Los Angeles.

Son personas interesadas en los aspectos más oscuros de los sistemas operativos, como pueden ser los agujeros de seguridad, y no solo en conocer esos agujeros, sino en conocer su por qué.

El problema es que esta afición, en principio perfectamente legítima, llevada a la práctica se mueve en los límites de la legalidad y es potencialmente muy peligrosa si las motivaciones de quien las realiza son malintencionadas, de ahí la mala fama de los hackers.

Un hacker, al contrario de la imagen pública que se tiene de ellos, tiene una serie de normas, algunas de índole ético, que son ampliamente conocidas en el entorno hacker ya que es lo primero que se le dice a alguien que quiere introducirse en dicho entorno.

Algunas de estas normas son el no hacer daño intencionadamente, modificar sólo lo estrictamente necesario para entrar y evitar ser localizado, no hackear nunca ni por venganza ni por intereses personales o económicos, así como no comentar con nadie las acciones realizadas.

Las características más comunes de personalidad son su alto nivel intelectual, gran curiosidad, y facilidad para abstracciones intelectuales.

Aunque una alta inteligencia en general es común entre hackers, hay otra característica más importante: la habilidad mental de absorber, retener, y referenciar grandes cantidades de detalles aparentemente sin importancia basados en la experiencia que le dan contexto y significado.

Son extraños en lo que se refiere al control y orden. Ellos tienden a tener el control absoluto de un sistema modificándolo a su propio gusto. Entre más control tengan de un sistema, más interés le atribuyen para poder mantenerlo siempre a ese nivel de eficiencia.

Para todo esto se necesita orden. Los hackers son intelectualmente ordenados. Muy meticulosos con lo que dicen o hacen.

Dentro de las comunidades hacker, se da más importancia a aquella que ha obtenido sus conocimientos de manera autodidacta ya que se considera mejor motivada que con la obligatoriedad de una escuela.

Las áreas académicas de mayor tendencia entre hackers son ciencias de la computación, ingenierías, física y matemáticas.

Los piratas jamás *trabajan* bajo su verdadero nombre, sino que emplean pseudónimos del tipo de "Mr. Smut", "Acidflux", "El Cowboy".

Un Hacker en general no se motiva con premios convencionales tales como la aprobación social o el dinero, sino que su mejor trofeo es haber logrado todo un desafío.

Su principal motivación es burlar la seguridad de los sistemas, pero no altera, destroza o cambia la información; sólo la observa.

Un hacker toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético que se describe a continuación:

El acceso a los ordenadores y a cualquier cosa que te pueda enseñar cómo funciona el mundo debería ser ilimitado y total. Siempre deberías poder ponerle las manos encima.

Toda la información debería ser gratuita. Si no tienes el acceso a la información necesaria para arreglar las cosas, ¿cómo vas a arreglarlas? Además, un intercambio libre de información permite una mayor  creatividad en general y evitar tener que reinventar la rueda una y otra vez.

Desconfía de la autoridad. Promueve la  descentralización. Lo mejor para favorecer el intercambio de información es un sistema abierto sin fronteras entre un "hacker" y la información que necesita.

Los "hackers" deberían ser juzgados por sus "hacks", no por criterios extraños como calificaciones académicas, edad, raza o posición. De hecho, uno de los "hackers" originales era Peter Deutsch, un niño de doce años que dominaba el TX-0 y que estaba por ello perfectamente integrado en el grupo.

Puedes crear arte y belleza en un ordenador, aunque aparte de la belleza en su sentido tradicional, los "hackers" creen que el código de un programa tiene una belleza propia, sobre todo cuando está escrito con maestría.

Los ordenadores pueden mejorar tu vida. Si sabes cómo pedírselo, un ordenador hace lo que tú le pidas, y  eso para los "hackers" representa la posibilidad de que cada usuario tenga a su disposición una herramienta poderosísima con la que puede hacer cualquier cosa que  desee.

Como vemos, la filosofía hacker nada tiene que ver con el vandalismo. Tal es así, que no resulta extraño que sea el propio hacker quien notifique al administrador los fallos de seguridad encontrados y la forma de solucionarlos, hasta el punto de producirse la *profesionalización,* creando empresas que, por encargo, asaltan ordenadores con el fin de detectar estos fallos.

En este trabajo la muestra consiste en nueve casos publicados y tres entrevistas relacionados con algunos comunes delitos informáticos. Los individuos seleccionados son todos varones, en su mayoría adolescentes, con altos niveles educacionales, económicos y culturales.

**Cracker**

Para las acciones nocivas existe la expresión, "cracker". Este término fue acuñado hacia 1985 por hackers en defensa contra la utilización inapropiada por periodistas del término hacker.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de software y hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutada automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Tienden a agruparse en grupos pequeños, muy secretos y privados. También se los ha llamado cyberpunks, sobre todo por la filosofía anti-sistema y porque muchas veces sabotean sistemas informáticos de grandes empresas que acumulan cuantiosos beneficios.

Los miembros de este grupo no tienen habilidades significativas en programación, no conocen términos extremadamente técnicos, ni tampoco tienen experiencia en plataformas Unix u otro verdadero sistema multiusuario.

Sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia. El cracker tiene como intención destruir.

Entre las variantes de crackers maliciosos están los que realizan *Carding* (tarjeteo, uso ilegal de tarjetas de crédito), o *Trashing* (basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos).

Los crackers, pueden ser empleados rencorosos o frustrados de alguna empresa, que tengan fines maliciosos o de venganza en contra de alguna empresa o persona, o pueden ser estudiantes que quieran demostrar sus habilidades pero de la manera equivocada o simplemente personas que lo hagan sólo por diversión.

**Phreaker**

Un phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

Estos sujetos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades -en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación-, pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de "Hacking" a sus servidores.

**d -** **Virucker**

Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

**5.2.3 – Instrumentos y materiales de evaluación**

Los instrumentos seleccionados para este trabajo de investigación son: un cuadro de identificación de casos desde lo jurídico y la incorporación de los datos de los delincuentes informáticos hasta donde fue posible.

**a) Identificación de casos desde lo jurídico**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Cuadro II – Identificación de casos desde lo jurídico** | | | | |
| **Año** | **Sobrenombre** | **Edad** | **Delito** | **Condena** |
|  |  |  |  |  |
|  |  |  |  |  |

En este cuadro se ubicaron, en cinco columnas, los principales datos de los casos seleccionados en los últimos años, a partir de la aparición de la red Internet.

En la primera columna se identifica el año y ha servido para determinar la evolución del fenómeno. La segunda columna hace referencia a los diversos apodos o sobrenombres que utilizan para ocultar su verdadera identidad. La tercera indica la edad cronológica de los sujetos, la cuarta señala el delito por el que fueron condenados y la quinta que, como culminación, describe la condena que se les impuso.

**b)** **Análisis de historias individuales**

A través de este instrumento se describen las principales características sintetizadas de los casos sobre delincuentes informáticos, que se obtuvieron a partir de consultas a la red Internet y a material publicado como diarios y revistas, donde se ubicó información que sirvió para componer una recopilación adecuada, clasificándolos a partir de su perfil delictivo en el uso de la redes de comunicación digitales.

**5.2.4 – Procedimientos**

Para producir el análisis de los datos recopilados nos hemos inclinado por tomar como referente práctico a la observación de historias de vida realizadas en torno a la obra de Liberman, donde enuncia los estilos comunicacionales, a los que encontramos relacionados en los casos recopilados en esta investigación.

**Capítulo VI**

**Análisis de los datos**

**6.1 – Identificación de casos desde lo jurídico**

Tal como se detalló en el capítulo anterior, este cuadro muestra de los casos seleccionados los que tienen una implicancia jurídica, a modo de síntesis del delito y sus respectivas condenas.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Cuadro II – Identificación de casos desde lo jurídico** | | | | |
| **Año** | **Sobrenombre** | **Edad** | **Delito** | **Condena** |
| 1980 | **Caso Nº 1:**  Estados Unidos  **Cóndor** | 16 | - Rompió la seguridad del sistema administrativo de su colegio no para alterar sus notas, lo hizo "sólo para mirar".  - Capaz de crear números telefónicos imposibles de facturar  - Apropiarse de veinte mil números de tarjetas de crédito | 3 meses de cárcel y un año de libertad condicional |
| 1981 |  | 17 | - Entró físicamente a las oficinas de COSMOS de Pacific Bell. La información robada tenía un valor equivalente a los doscientos mil dólares. |  |
| 1982 |  | 18 | - Entró ilegalmente, vía módem, a la computadora del North American Air Defense Command en Colorado |  |
| 1983 |  | 19 | - Entró ilegalmente a ARPAnet  (La predecesora de Internet) y trató de acceder a la computadora del Pentágono.  - Acusado de invadir el sistema de la compañía Microcorp Systems. |  |
| 1987 |  | 23 | - Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia. |  |
| 1988 |  | 24 |  | 6 meses de cárcel en una prisión juvenil |
| 1991 |  | 27 |  | Tres años de libertad condicional luego de la sentencia su expediente desapareció de la computadora de la policía local. |
|  |  |  |  | Un año de prisión y al salir de allí a un programa de seis meses para tratar su "adicción a las computadoras". |
| 1995 | **Caso Nº 2:**  Argentina  **El Gritón** | 21 | -Tuvo acceso a documentación "sensible pero no calificada", sobre el diseño de radares y aviones militares.  - Se infiltraba en la red de computadoras de la empresa Telecom a través de líneas telefónicas 0800 de uso gratuito. | EE.UU:  Tres años de libertad condicional y a pagar una multa de cinco mil dólares  ARG:  condenado a cumplir con un servicio social -dar clases de computación en instituciones públicas- y a pagar una multa de 50 pesos por fraude telefónico. |
| 1981 | **Caso Nº3:**  Estados Unidos  **Capitán Zap** | 23 | - Entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum. | - Multado por U$S 1000 y sentenciado a 2 años y medio de prueba. |
| 1986 | **Caso Nº4:**  Estados Unidos  **Shadowhack** | 16 | - Violó el acceso a AT&T y los sistemas del Departamento de Defensa de EE.UU. | - Sentenciado a 9 meses de cárcel y a una fianza de U$S 10,000 |
| 1988 | **Caso Nº5:**  Estados Unidos  **Morris, Robert** | 18 | - Diseñó un programa gusano | - Tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza |
| 1998 | **Caso Nº6:**  Argentina  **X-Team** | s/d | - Irrumpieron en la página web de la Corte Suprema de Justicia Argentina reclamando la solución urgente del crimen del periodista José Luis Cabezas. | No hubo |
| 2000 | **Caso Nº7:** | 16 | - Irrumpir en los servidores de la National Aeronautics and Space Administration, NASA. | 6 meses de cárcel |

Cuadro de la autora. 2005.

**6.2 – Presentación de casos**

**Caso Nº 1: Kevin Mitnick. Alias “Cóndor”. 16 años- EE.UU. Año: 1980.**

Fuente: Pág web kevinmitnick.com y del libro de Markoff, John y Hafner, Katie. *Cyberpunk*, pág 122.

Fue capaz de crear números telefónicos imposibles de facturar.

Capaz de apropiarse de veinte mil números de tarjetas de crédito de habitantes de California.

Burlarse del FBI por más de dos años con sólo un teléfono celular alterado y una computadora portátil.

Delito: Fue sospechoso de robar el software de más de media docena de fabricantes de teléfonos celulares.

Tenía el control de tres oficinas centrales de teléfonos en Manhattan (New York) y de todos los centros de conmutación de California. Esto le daba la habilidad de escuchar cualquier conversación telefónica; y si no eras una persona de su agrado, modificar el teléfono de tu casa, de tal manera que cada vez que levantaras el teléfono una grabadora pedía ingresar veinticinco centavos.

*Carrera informática delictiva de Mitnick*

Inicios en 1980. Tenía 16 años. Rompió la seguridad del sistema administrativo de su colegio, pero dijo “no para alterar las notas” lo hizo sólo “para mirar”.

En 1981, entró físicamente junto a dos amigos a las oficinas de COSMOS (Computer System for Mainframe Operations), una base de datos usadas por casi todas las compañías telefónicas norteamericanas.

En esta ocasión, a sus 17 años obtuvieron la lista de claves de seguridad y la combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS. La información robada tenía un valor equivalente a los doscientos mil dólares.

Fueron delatados a las autoridades por la novia de uno de sus amigos, y debido a su minoría de edad fueron a una Corte Juvenil que lo sentenció a tres meses de cárcel y un año bajo libertad condicional.

Como respuesta, luego de los tres meses de cárcel, el oficial custodio encargado de su caso encontró que su teléfono fue desconectado y que en la Compañía Telefónica no tenían ningún registro de él.

En 1982, entró ilegalmente vía módem a la computadora de la Fuerza Aérea Norteamericana. Antes de entrar en la computadora, alteró el programa encargado de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar.

El FBI creyendo haber encontrado a Mitnick, allanó la casa de unos inmigrantes que estaban viendo televisión.

En 1983, con 19 años, fue detenido cuando era estudiante de la Universidad del Sur de California. Entró ilegalmente a Arpanet (la predecesora de Internet) y trató de acceder a la computadora del Pentágono. Por esto lo sentenciaron a seis meses en una prisión juvenil.

En 1987 fue acusado de invadir al sistema de la Compañía Microcorp Systems. Lo sentenciaron a tres años de libertad condicional. Y como respuesta hacker, luego de la sentencia, su expediente desapareció de la computadora de la policía.

Mitnick solicitó empleo como encargado de la seguridad de la red de un banco. El banco lo rechazó por sus antecedentes penales. Como respuesta, Mitnick falsificó un balance general del banco que mostraba pérdidas importantes, y trató de enviarlo por la red. Afortunadamente el administrador de la red detuvo el balance antes que fuera enviado.

Durante meses observó secretamente el correo electrónico de algunos miembros del Departamento de Seguridad de MCI, una importante empresa de comunicaciones americana. Luego de recoger suficiente información, se apoderó de 16 códigos de seguridad y junto a un amigo entraron a la red del laboratorio de investigaciones de Digital Corporation para obtener una copia del prototipo del nuevo sistema operativo de seguridad. El personal de seguridad de Digital, se dio cuenta del ataque y avisó al FBI y rastrearon a los hackers.

Mitnick fue un mal cómplice y trató de culpar a su amigo, haciendo llamadas anónimas al jefe de éste, que trabajaba en una compañía de software. El amigo le confesó todo a su jefe, quien los denunció a Digital y al FBI.

Lo sentenciaron en 1988 por invadir el sistema de Digital Equipment y el robo del sistema operativo. Los daños fueron valuados en cuatro millones de dólares.

Fue declarado culpable de un cargo de “fraude en computadoras” y de uno por “posesión ilegal de códigos de acceso de larga distancia”.

Le prohibieron el uso del teléfono en prisión.

El abogado de Mitnick convenció al juez que sufría de una “adicción a las computadoras” equivalente a la de un drogadicto, alcohólico o un apostador.

Gracias a esta maniobra de la defensa, Mitnick fue sentenciado a sólo un año de prisión y que, al salir de allí, debía seguir un programa de seis meses para tratar su adicción a las computadoras.

Durante su tratamiento le prohibieron tocar una computadora, o un módem; y llegó a perder 45 kilos.

En 1991 luego de concluir su programa, ya era el hacker que había ocupado la primera plana del New York Times, y uno de sus periodistas escribió un libro estilo *cyberpunk* narrando las aventuras de Mitnick. Al parecer el libro no le gustó, ya que luego de ser publicado, la cuenta de correo del periodista fue invadida, cambiando su nivel de acceso; de tal manera que cualquier persona en el mundo que estuviera conectada a Internet podía ver su correo electrónico.

En 1992 Mitnick comienza a trabajar en una agencia de detectives. Pero se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI, que determinó que había violado los términos de la libertad condicional.

Allanaron su casa, pero había desaparecido sin dejar rastro alguno.

Un tiempo después, el Departamento de Vehículos de California ofreció una recompensa de un millón de dólares a quien arrestara a Mitnick.

Trató de obtener una licencia de conducir de manera fraudulenta, utilizando un código de acceso y enviando los datos vía fax.

Mitnick como prófugo de la justicia, cambió de táctica y empezó a utilizar teléfonos celulares ya que consideraba que era la mejor manera de no ser rastreado.

En navidad de 1994 invadió la computadora personal de Shimomura, físico computista y experto en seguridad del Centro de Supercomputadoras de San Diego en California. Este es a la vez un gran hacker, aunque era uno de los “chicos buenos” (white hat), quienes cuando descubren una falla en la seguridad de algún sistema se lo dicen a las autoridades, y no a otros hackers. Mitnick robó de la computadora de Shimomura su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet.

En 1995 el software de Shimomura fue encontrado en una cuenta en “The Well”, un proveedor de servicios de Internet en California.

Mitnick había creado allí una cuenta fantasma y desde allí utilizaba las herramientas robadas para lanzar ataques a corporaciones de computadoras (Apple, Motorola).

En esta ocasión, había creado una cuenta de nombre Nancy, borrado una con el nombre Bob y había cambiado varias claves de seguridad, incluyendo la de los expertos y los que tenían privilegios más altos. Había invadido también Netcom, una base de datos de noticias.

El FBI comenzó la búsqueda por radio, con un equipo de rastreo. Este poseía un simuladora de celda, un equipo normalmente utilizado para probar teléfonos celulares, pero modificado para rastrear el teléfono de Mitnick mientras esté encendido y aunque no esté en uso. Con este equipo, el celular se convertía en un transmisor sin que el usuario lo supiera.

El FBI no buscaba a un hombre, buscaba una señal. Una vez que localizaron su señal, Shimomura mandó un mensaje varias veces por error, al encargado de seguridad de Netcom, que decía que la captura iba a ser al día siguiente.

El encargado interpretó que Mitnick ya había sido arrestado adelantándose a realizar una copia de respaldo (backup) de todo el material que Mitnick había almacenado en Netcom como evidencia, y borrando las versiones almacenadas por Mitnick.

Tenían que atraparlo antes que Mitnick se diera cuenta que su información había sido borrada. Cuando el FBI encontró a Mitnick en un departamento, éste abrió la puerta con toda calma.

Arrestado Mitnick, Shimomura regresa a su casa en San Diego, y encuentra en la contestadora telefónica de su casa, varios mensajes que Mitnick le había dejado con acento oriental en tono de burla. Lo curioso es que el último de estos mensajes lo recibió ocho horas después de que Mitnick había sido detenido.

Lo sentenciaron a dos cargos federales en Estados Unidos, “uso ilegal de equipos de acceso telefónico” y “fraude por computadoras”. Todos los cargos podían suponerle más de doscientos años en la cárcel. Pero Mitnick pagó la fianza y salió bajo libertad condicional. *Perfil del Caso: Hacker, phreaker, cracker.*

**CASO Nº 2: Julio César Ardita. Alias “El Gritón”. 21 años. Argentina. Año: 1995.**

Fuente: Pág. Web [terra.com.ar/](http://www.terra.com.ar/) tecnología

El Día de los Inocentes de 1995, (28 de diciembre), la casa de este joven fue allanada por la justicia argentina, luego de que el Gobierno de Estados Unidos alertara sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Utilizando las líneas 0800 de uso gratuito de Telecom Ardita logró acceder al sistema de redes de la Universidad de Harvard y desde allí, a información sobre el diseño de radares y aviones militares.

El fiscal de la causa le dijo a periodistas que la soberbia de Ardita lo llevó a admitir todos y cada uno de los hechos que se le imputaban.

Lo sentenció un tribunal oral en 1996, por “fraude telefónico”, estimado por la empresa Telecom en cincuenta pesos.

Este fue el primer juicio de estas características en Argentina. En 1995, en Argentina, el acceso a la red Internet -que hoy es muy común-, era un privilegio, sólo para muy pocos.

Por eso, detallar en un juzgado qué era la red, cómo consiguió concretar a través de Internet, comunicaciones internacionales desde su casa sin pagar un solo centavo, fue una tarea dura para Ardita, que necesitó gráficos para explicar cómo ingresó a la red interna de computadoras de Telconet (de Telecom) a través de una línea 0800.

Sin embargo, para acceder a esta red es necesario poseer una clave secreta de catorce dígitos. Cada usuario legítimo tiene una, por eso fue que al principio la investigación apuntó que algún contacto dentro de la empresa telefónica le hubiera facilitado el código.

Pero para Ardita las cosas habías sido más simples: “Cuando uno establece la conexión Telconet y presiona simultáneamente las teclas “ctrl.-p” y luego tipea “stat”, el sistema da mucha información”. La denominación STAT es tomada por el sistema informático como “status” y pone en pantalla la información de los últimos accesos de personal validado por el sistema, con sus nombres de usuario y sus claves secretas. Cuando sorteó la primera valla de seguridad, descubrió la red de computadoras que Telecom tenía conectada a Internet. Sólo que para ingresar era necesario ser usuario legal, por lo tanto explicó que: “Comencé entonces a probar diferentes nombres de personas: María, Julio, etc. Pero recién con el nombre Carlos obtuve respuesta”. Así, a través del sistema de prueba y error navegó gratis por Internet, y ahí comenzaron sus problemas con la ley norteamericana, ya que desde allí ingresó al sistema de la Universidad de Harvard, que a su vez le sirvió de trampolín para acceder a los de la Marina de los EE.UU., y del laboratorio de Propulsión Nuclear de la NASA, entre otros.

En esa época, para los EE. UU. las intrusiones informáticas ya eran delitos graves. Así, un tribunal condenó a Ardita a tres años bajo libertad condicional y a pagar una multa de cinco mil dólares por haber vulnerado el sistema informático de la Marina.

En el juicio de Boston, realizado allí porque es donde se encuentra instalada la Universidad de Harvard, lo condenaron puntualmente por “posesión fraudulenta de claves de seguridad, nombres de abonados legítimos, códigos y otros permisos de acceso, por actividad fraudulenta y destructiva con computadoras y por interceptación ilegal de comunicaciones".

Ardita obtuvo información sobre tecnología espacial y aérea, y entró a sistemas de universidades donde se hacían investigaciones sobre satélites y radiación.

El agente especial del FBI Black, vino a Argentina para capacitar a la Policía Federal y le dijo a un periodista: “El hacker argentino operaba desde 4 ó 5 cuentas distintas (números de usuario) que pertenecían a la universidad de Harvard. Cambiaba de una a otra y por eso fue difícil detectarlo.

No hubo pruebas de que Ardita haya intentado lucrar con la información o hacer algún tipo de daño.

Por eso fue condenado a cumplir con un servicio social: dar clases de computación en instituciones públicas y pagar una multa de 5.000 dólares.

Ardita junto a un socio capitalista fundó una empresa de seguridad en informática a los 25 años.

HACKER: Ardita considera que esta palabra ha sido deformada. El verdadero significado tiene que ver con alguien que se dedica a investigar en cualquier aspecto de la vida.

*Perfil del Caso: Hacker.*

**CASO Nº 3: Ian Murphy. Alias “Captain Zap” 23 años. Año: 1981**

Fuente: Pág web mailxmail.com

Entra a los sistemas de la Casa Blanca, el Pentágono, Bell South Corporation y TRW y deliberadamente deja su CV.

En ese año todavía no había leyes muy claras, aún en EE.UU.

Este caso mostró la necesidad de hacer más clara la legislación cuando, con tres amigos, usando una computadora y una línea de teléfono desde su casa, violaron los accesos restringidos, consiguiendo tener acceso a órdenes de mercancías, archivos y documentos del gobierno.

La banda de hackers terminó con cargos por robo de propiedad. A Murphy, una multa de mil dólares y fue sentenciado a dos años y medio de prueba.

*Perfil del Caso: Hacker.*

**CASO Nº 4: Zinn, Herbert. Alias “Shadowhack”. 16 años. 1986.**

Fuente:Pág web mailxmail.com

Fue el primer sentenciado bajo el cargo de fraude computacional y abuso. Violó el acceso a AT&T y los sistemas del Departamento de Defensa de los EEUU.

Fue sentenciado en 1989 por la destrucción del equivalente de 174.000 dólares en archivos y copias de programas. Además publicó contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales.

Lo condenaron a 9 meses de prisión, y a pagar una fianza de 10.000 dólares. Se estima que si hubiera tenido 18 años en el momento del hecho, la sentencia hubiera podido alcanzar 13 años de cárcel y una fianza de 800.000 dólares.

*Perfil del Caso: Hacker y cracker.*

**CASO Nº 5: David Smith, programador de 30 años.**

Fuente: Pág web mailxmail.com y del libro de Palazzi *Delitos informáticos, pág 134.*

Fue detenido por el FBI acusado de crear y distribuir el virus “Melissa”, que bloqueaba las cuentas de correo electrónico.

Los cargos fueron por bloquear las comunicaciones públicas y dañar los sistemas informáticos. La pena podía ser de hasta 10 años en prisión, pero en realidad salió en libertad bajo fianza de 10.000 dólares.

El virus Melissa contaminó a más de 100.000 computadoras de todo el mundo, afectando a empresas como Microsoft, Intel y Compaq.

En España hubo una campaña de información en TV alertando a los usuarios sobre este virus.

¿Quiénes lo buscaron?

Fue buscado por el FBI y técnicos del proveedor de servicios de conexión a Internet de EEUU, America On Line; porque para propagar este virus Smith había utilizado la identidad de un usuario de su servicio de acceso.

La detención de Smith, sin embargo, no significa que el virus haya dejado de actuar.

*Perfil del Caso: Virucker.*

**CASO Nº 6: Wau Holland y Steffen Wenery. 1987.**

Fuente: mailxmail.com

En 1987 dos hackers alemanes de 20 y 23 años ingresaron sin autorización al sistema de la central de investigaciones aeroespaciales más grande del mundo, la NASA.

Ellos les mandaron un mensaje, avisaron y pararon el juego. No fueron sentenciados. Con esos datos Steffen anulaba la intención de presentar a los hackers como sujetos peligrosos para otros.

*Perfil del Caso: Hacker.*

**CASO Nº 7: Robert Morris. Año: 1988**

Fuente: Palazzi Pablo *Delitos informáticos, pág 187*

Lanzó un programa “gusano” diseñado por él mismo, para navegar en Internet, buscando debilidades en sistemas de seguridad y que pudiera correrse y multiplicarse por sí solo. Por su causa más de seis mil sistemas resultaran dañados.

Eliminar el gusano de sus computadoras causó a las víctimas muchos días de improductividad y millones de dólares perdidos.

Por este motivo los servicios policiales estatales estadounidense crearon el Equipo de Respuestas de Emergencias Computacionales (CERT), para combatir problemas similares en el futuro.

Morris, fue sentenciado y condenado a tres años de libertad condicional, 400 horas de trabajo comunitario y pagar una fianza de 10.000 dólares, bajo el cargo de “fraude computacional y abuso”. Pero la sentencia fue criticada de ligera, pero reflejaba lo inocuo de las intenciones de Morris, más que el daño causado.

Este gusano no borra ni modifica archivos en la actualidad.

*Perfil del Caso: Virucker.*

**CASO Nº 8: Poulsen, Kevin. Alias “Dark Dante”. Año: 1992.**

Fuente: Pág web mailxmail.com

Es acusado de robar información vía computadora: órdenes de tarea relacionados con un ejercicio de la fuerza aérea militar norteamericana.

Fue también perseguido varios años por el FBI y al fin apresado, juzgado y condenado.

Conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a “ganar” un Porsche en un concurso radiofónico, si su llamada era la 102, y así fue. También crackeó todo tipo de sitios web, pero le interesaban los que contenían material de defensa nacional.

Estuvo cinco años en prisión, fue liberado en 1996, supuestamente reformado. Este es el mayor tiempo que ha estado un hacker preso.

*Perfil del Caso: Phreacker, Cracker.*

**CASO Nº9: “X-Team”. Año: 1998.**

Fuente: Pág web terra.com

El primer grupo de piratas informáticos argentino dedicado a las intrusiones de carácter político, su líder fue Julio López, Alias “Wences”.

En ese año, irrumpieron en la página web de la Corte Suprema de Justicia Argentina reclamando la solución urgente del crimen del periodista José Luis Cabezas.

¿Quién los denuncia?

El presidente de la Corte Suprema.

Fallo: “Una página web no puede asimilarse al significado de cosa”. Titular del Juzgado de Buenos Aires.

El abogado defensor: “No hay leyes para sancionar el sabotaje informático”.

Pero no todos los expertos del Derecho coincidieron con el juez.

El abogado de Microsoft, criticó el fallo, según él se atentó contra un bien material o cosa, que es la memoria donde está grabado el archivo html. (que cuando se ejecuta produce el despliegue del sitio o pág web).

Los hackers cambiaron la combinación de unos y ceros que la conforman.

La causa por el ataque a la página web, no presentó grandes novedades hasta fines del 2000.

A partir de este caso fue creada recientemente la División de Informática Criminal de la Policía Federal Argentina. Su actuación en el caso estuvo plena de irregularidades. Cinco meses después el caso terminó con la absolución de todos los imputados.

**CASO Nº 10:** **Entrevista 1**

Fuente: Pág Web datosenlaweb.com

¿Qué es un hacker?

Una persona que investiga la tecnología de una forma no convencional. La definición más popular de hacker es la del señor que viola sistemas de computadoras.

¿Quién no es un hacker?

Todos los demás, el que no viola los sistemas de seguridad. “En esa época no había muchas cosas disponibles para la gente, lo que había era sólo para empresas, entonces vos querías jugar con eso”. La actitud es divertirse con la tecnología, vas encontrando cosas, y a partir de ahí seguís jugando.

¿Hay hackers buenos y hackers malos?

Tendrían que dividirse en función de la intención."Hackear es un hobby". El tipo que está hackeando con un objetivo en mente, está usando el hacking como medio para llegar a otra cosa.

Fui el primero que se animó a hablar del tema. Fundamentalmente para distinguir hackear como investigar y probar límites de seguridad o como para un beneficio previamente pensado que utiliza el hacking como técnica para conseguir información determinada, con intención subyacente. “Yo para laburar doy consultoría”. "He asesorado a la justicia".

Su definición de hacker: “Se define en función de las cosas que hacés. El hacker admirable es el que le da un uso brillante a la tecnología, un uso novedoso, que a nadie se le hubiera ocurrido”.

**CASO Nº 11: Entrevista 2**

**Entrevista a ex hacker. Alias “Chacal”.**

Fuente: Pág Web ubik.to

En la actualidad tiene alrededor de 30 años. Es dueño de una empresa de consultoría en el área de informática, vinculado con comunicaciones y redes.

“Cuando era más joven me dedicaba al hacking, creo que ese es el motivo de esta entrevista”.

“El pico de la actividad fue en el año 1987, yo tenía veintialgo. Era otra etapa de la vida, en la que tenías tiempo para dedicarle a este tipo de cosas”.

"Lo dejé porque es una actividad que lleva mucho tiempo; pude reestructurar todos los conocimientos que adquirí en esa etapa de hacking. Los he capitalizado para dedicarlos a la actividad productiva, y no al hacking que es en sí un hobby, una diversión".

Su definición de hacker

El concepto popular: “persona que accede a otras computadoras en formas no muy oficiales, rondando o no la ilegalidad, depende como se lo considere".

Es el personaje popularizado por películas como “Juegos de Guerra”. "La actividad del hacker es investigar donde puede entrar, cómo entrar, cómo violar la seguridad de los mecanismos de acceso a las comunicaciones por satélite, a las universidades, a las empresas o centros gubernamentales en el exterior".

"Una vez allí es más que nada una actividad vouyerística, un juego de ajedrez intelectual contra la seguridad del sistema que se pretende violar”.

“Es ingresar, mirar y nada más. La intención del hacker no es destruir información. El objetivo nunca es destruir, porque el hacker quiere pasar desapercibido. Es una satisfacción intelectual. Se comparte con un círculo de iniciados”.

“En cierto modo es lo mismo que preguntar quien es el mejor especialista en cajas fuertes: es el ladrón de cajas fuertes. Es el que más va a saber cómo hacer una inviolable. Conocimientos aplicados para hacer lo contrario".

“No deja de ser parte de este juego de ajedrez, nada más que al principio se juega de un lado del tablero y ahora del otro: antes el juego era violar los sistemas, y ahora es crear sistemas seguros y brindar ese servicio a las empresas”.

"A nivel grupal, PUA Piratas Unidos Argentinos: son hackers conscientes, esa conciencia surgía por la necesidad de haber trabajado mucho a pulmón. En ese momento existían diferentes lugares secretos en la red. Algunos ciertos, otros de fantasía. Esos lugares eran computadoras escondidas en las redes mundiales de comunicaciones". "Allí se intercambiaba información: códigos de acceso, etc. (ALTOS, AMP, QSD) Adventure Multiplayer". "La información se intercambiaba mediante juegos de aventura multiusuarios, chats".

"El hacker bien entendido es una especie de Robin Hood de la información, que permite que todo el mundo acceda a información que de otra manera se mantiene oculta".

Su opinión sobre la personalidad hacker: "Hay muchos que se aíslan de la realidad, lo cual puede ser válido o no.

El perfil en general es una persona con profundos conocimientos técnicos, es un nuevo marginado, un nuevo bohemio, un nuevo artista". "Va a estar más inclinado a hackear un sistema con la PC que a ir a un partido de fútbol con sus compañeros de la facultad o de la secundaria”. "Es probable que tenga ciertas inclinaciones locas, como recitales o practicar un deporte peligroso como paracaidismo o aladeltismo". "Hoy en día el hacker ya se fue incorporando al tejido de la sociedad y podemos encontrar hackers de todo tipo. Es difícil definir un perfil único de hacker”.

Opinión sobre las edades de los hackers: "El hacker se inicia durante la adolescencia, porque en ese momento tiene la capacidad intelectual para dedicarse al tema y dispone de tiempo".

Opinión sobre los virus: "La idea de virus surgió simultáneamente en muchos lugares del mundo. Nunca se me ocurrió la idea de hacer un virus que destruyera información. La idea era crear un programa vírico que mostrara mensajes, que dijera algo".

-¿Algo así como el Ping Pong?

"En ese momento no teníamos conciencia de que un virus supuestamente inofensivo pueda crear incompatibilidades o no entenderse con otros programas importantes como un caché o un controlador de memoria y crear desastres accidentalmente". "Creo que es consecuencia de la mentalidad un poco megalomaníaca del adolescente frustrado, que es el perfil típico del creador de virus". "Es el adolescente frustrado que de esa manera llena su ego sintiéndose una persona importante, porque crea un virus que después destruye millones de datos". "Las mismas técnicas de programación que se usan para desarrollar un virus pueden servir para muchas cosas; con el virus existe el riesgo que pueda escapar de las manos del programador". "La intención de destruir información es inútil. Ese es el límite entre la travesura y la actividad criminal".

- Ahora tenés una posición más legalista y seria. Hace unos años, cuando eras hacker, ¿pensabas de la misma forma o eras un poco más anarquista?

"Era un poco mas anarquista. Todavía estoy a favor del libre flujo de información. Creo que es importante que la gente pueda acceder a la información, que las computadoras y las comunicaciones entre las computadoras permitan, como lo decía McLuhan, la aldea global".

"Era un poco romántico lo que hacíamos en esa época, era un desafío con ciertas reglas de caballerosidad. Éramos caballeros de las redes de comunicaciones".

"Es lo mismo que sucede con cualquier actividad: cuando eso se masifica, empieza a haber todo tipo de personas, buenos, malos, y se pierde muchas veces el sentido original".

“Es como jugar al ajedrez haciendo trampa o pegándole con las piezas en la cabeza al contrincante, no tiene ninguna gracia. La gracia está en ganar respetando las reglas del juego. Esto es lo mismo, las reglas del juego son: romperse la cabeza para conseguir la información, lograr acceder y actuar caballerosamente, igual que un buen jugador de ajedrez".

**CASO Nº 12: Entrevista 3**

Fuente: Esta entrevista fue realizada por Jorge Machado de Perú, en la 4a Convención de Hacker On Planet Earth, el 16 de Julio de 2002. Pág web Ulpiano.com

Año 2000. A los 16 años irrumpió en los servidores de la NASA. Lo condenaron a seis meses de detención en una prisión juvenil.

-¿Qué tienen las computadoras que los obsesiona?

“Es el poder en la punta de tus dedos. Puedes controlar todas esas computadoras, desde las del gobierno, las militares y las de las grandes corporaciones. Es un viaje de poder. Sentirse dueño del control. Es intelectual. Estimula la mente. Es un reto”.

-¿Qué tan difícil fue ingresar en algunas de las computadoras del gobierno?

"Ellos están desprovistos de ciertas serias medidas de seguridad".

-¿Y cómo aprendiste eso?

“Leyendo, hablando con la gente que conocía, pasando mucho tiempo en la computadora”.

-¿Ustedes comparten o intercambian técnicas de hacking y las vulnerabilidades de Internet?

"Sí, por supuesto. Los sitios desprotegidos no me llaman la atención, en cuanto puedo crackearlos en unos cuantos minutos. Yo apuntaba a un lugar porque significaba un gran reto”.

-Pero eso suena como una travesura. A veces pienso que Uds. son como los pintores de graffiti con spray.

"Hay otros que ingresan a sitios web y cambian los portales. Esas son travesuras. Personalmente no me gusta hacer cosas así".

-Pero podrías hacerlo...

"Sí. Yo pude obtener algo de respeto y mucha consideración".

-Se le prestó mucha atención al hecho que descargaste software relacionado a la NASA. ¿Pudiste hacer algo con eso?

"No. La única razón por la cual yo descargué el software, se debió a que estaba estudiando programación en Lenguaje C. ¿Qué mejor forma habría que leer el software escrito por el gobierno? A ellos no les importa que yo esté allí. Les dí consejos y nunca me hicieron caso".

-¿Cómo te encontraron?

"Probablemente contactaron y amenazaron a uno de mis amigos. El FBI fue a mi casa. Les conté cómo lo hice y lo que hice. Ellos me dijeron que no lo volviera a hacer y si lo hacía, me llevarían con esposas, pero por el momento no me consideraron un criminal".

-¿Se llevaron algo de tu casa?

"Cinco de mis computadoras, mi Palm Pilot, mis CDs y mi libro de Star Treck".

-Pensemos desde el punto de vista de la otra parte. Ellos no sabían que se trataba de un joven educado de un barrio elegante. Podrías haber sido un verdadero tipo malo en Bagdad, o donde sea, ¿qué es lo que se supone que deben hacer cuando descubren que alguien está fisgoneando en sus sistemas?

"Ellos deberían ser suficientemente responsables para proveer de una adecuada seguridad a sus sistemas. Pero ellos no deberían poner en la cárcel a un joven de los EE.UU. de América".

-¿Cómo te afectó la posibilidad de ir a la cárcel por seis meses?

"Y... yo me estoy sometiendo ante esa gente que es más baja que yo. Que no suene arrogante, pero a ellos les falta moral. Y sería degradante para mi persona... y estoy preocupado".

-¿Estas tratando de decirme que no piensas que el delito que cometiste no es de la misma naturaleza?

"Esta es una exploración no perjudicial. No es un acto violento o destructivo. Es nada".

-Ellos dicen en un punto, que tomaste posesión de un valor de un millón de dólares en software, que hiciste paralizar durante semanas trece ó catorce servidores de computadoras del Gobierno. Eso suena grave...”

"Yo pienso que el precio del software es irrelevante. Era código fuente que ni siquiera pudo haber sido compilado con el equipo apropiado o quizás estaba mal codificado, yo no comprendo... pero la única razón por la cual descargué ese software fue a causa del aprendizaje, para saber lo que ellos estaban haciendo, la forma como programaban, sus técnicas".

-¿Y aprendiste básicamente que eso no era bueno?

"Sí. Ellos se hicieron los estúpidos, cosas estúpidas que los programadores experimentados no deberían hacer. Le llaman daños cuando un entusiasta de las computadoras como yo, les demuestra su ineptitud".

-¿Cómo evaluarías los niveles de habilidad de la gente de las fuerzas estatales que eventualmente llegaron a tocar a tu puerta?

"Yo no cubrí todas las pistas del todo, y si lo hubiese hecho, ellos jamás habrían tenido la capacidad de capturarme".

-¿Podrías haber causado un mayor daño?

"Podría haber borrado archivos, o colocar un virus o vender la información a países extranjeros. Podría haber ejecutado una negación de servicio y causar que las redes de computadoras queden fuera de funcionamiento. Alguien podría haber realizado una enorme cantidad de cosas que yo no hice".

-¿Podrías haber hecho esas cosas?

"Sí. Podría haberlo hecho".

-¿Qué vas a hacer ahora?

"Quizás empiece a formar una compañía de seguridad en computadoras".

**6.3- Análisis de los grupos identificados como muestra**

El siguiente análisis intenta definir a cada grupo, mostrar las principales características de personalidad y de estilos comunicacionales, motivaciones, percepción de identidad, grado de peligrosidad y ética.

**6.3.1 - Psicología Hacker y Phreaker**

En el diccionario de términos informáticos, se define el término hack con las siguientes acepciones: 1. Nueva disposición inteligente y poco usual de los recursos existentes del sistema o red que produce, como por arte de magia, una mejora notable en el rendimiento del sistema, o una jugarreta casi igual de sorprendente. Un hacker es quien usa las computadoras para producir estos efectos y no es, necesariamente, un criminal informático. 2. Un trabajo “rápido y práctico” que produce resultados, pero sin seguir ningún procedimiento lógico u ordenado.

A la persona que utiliza el hacking, se la denomina hacker, y su definición tiene las siguientes acepciones: 1. Entusiasta aficionado a las computadoras cuya diversión estriba en aprender todo acerca de un sistema de computación o red y, mediante una programación hábil, llevar el sistema al nivel máximo de rendimiento. 2. La prensa lo utiliza como sinónimo de cracker. 3. Programador experto.

Estas personas suelen ser auténticos genios de la informática, que ingresan sin permiso en ordenadores y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita.

La organización susceptible de ser atacada por un hacker tiene que cumplir con la condición de poseer algo que le interese. Si no, aunque pudiera ser accesible a su conocimiento, simplemente no perderá el tiempo. Así pues, no es difícil imaginar que las empresas de comunicaciones, software e informática en general sean las preferidas por los hackers.

Entre los casos seleccionados de hackers la definición que ellos dan sobre este término, la motivación subyacente y la manera de realizar esta actividad se fragmenta a continuación:

Como hacker, la carrera de Mitnick alias “El cóndor” tiene sus inicios en

1980 cuando contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, sino que aseguró que lo hizo "sólo para mirar".

El Gritón: en 1995 se colgó de las redes de Telecom en Argentina y de

allí logró acceder a la Universidad de Harvard, a la Marina de Estados Unidos y al Pentágono. Tuvo acceso –con veintiún años- a documentación "sensible pero no calificada", sobre el diseño de radares y aviones militares norteamericanos.

"Cuando uno establece la conexión con la Telconet y presiona simultáneamente las teclas 'Ctrl-p' y luego tipea 'STAT', el sistema da mucha información", confesó. La denominación 'STAT' es tomada por el sistema informático como "status" y pone en pantalla la información de los últimos accesos de personal validado por el sistema, con sus nombres de usuarios y sus claves secretas.

“El objeto de todas mis incursiones en Internet fue la investigación”.

El hacker argentino operaba desde cuatro o cinco "cuentas" (números de usuario) que pertenecían a la Universidad de Harvard. Cambiaba de una a otra y por eso fue difícil detectarlo.

Considera que el verdadero significado del término hacker tiene que ver con alguien que se dedica a investigar, a tratar de sacar el máximo provecho no sólo dentro de lo informático, sino en cualquier aspecto de la vida.

“Un hacker es una persona que investiga la tecnología de una forma no

convencional. El pibe que desde chico empieza a desarmar el autito, es un hackercito.

A ese hay que cuidarlo, no se conforma en jugar como se debe. El tipo que está hackeando con un objetivo en mente, yo no sé si está hackeando. Está haciendo otra cosa y está usando el hacking como medio para llegar a otra cosa”.

El Chacal: “El concepto popular del hacker es que es la persona que

accede a otras computadoras en forma no muy oficiales, rondando o no la ilegalidad”.

“La actividad del hacker es investigar dónde puede entrar, cómo entrar, cómo violar la seguridad de los mecanismos de acceso a las comunicaciones por satélite, a las universidades, a las empresas o centros gubernamentales en el exterior. Una vez que está allí es más que nada una actividad voyeurística, un juego de ajedrez intelectual contra la seguridad del sistema que se pretende violar. Es ingresar, mirar y nada más. La intención del hacker, por lo menos del hacker bien entendido, no es destruir información, eso es un poco infantil. Acceder a un sistema para destruir información de pobres inocentes que no participan en el juego no tiene ninguna gracia”.

“El objetivo nunca es destruir, porque el hacker quiere pasar desapercibido. Es una satisfacción intelectual, que se comparte con un círculo de iniciados. Tiene esa característica un poco mística”.

“Hoy en día está mucho más vulgarizado, y hay un montón de pseudo-hackers que obtienen información de algún amigo que sabe un poquito más, les pasan una serie de archivos completos, entran, no saben cómo, no saben qué es lo que hacen, y eso no tiene gracia”.

“Los usuarios son muy poco conscientes de la posibilidad de que otra persona les descubra sus claves. Investigando un poco, probando, con muchas horas, con mucho tiempo, mucho trabajo, uno va llegando. Y a medida que uno accedía al extranjero, empezaba a entrar a círculos de hackers de todo el mundo donde se intercambia información”.

“Así, sabiendo mucho de sistemas, se buscan archivos que dan una pista de cómo está comunicándose esa computadora y se intentan utilizar los mismos mecanismos. Entonces se entra a esa computadora de Alemania haciéndose pasar por la computadora de Japón y así se va armando una cadena donde se van encontrando cosas a las que acceder”.

“Llevándolo a un plano idealista, el hacker bien entendido es una especie de Robin Hood de la información, que permite que todo el mundo acceda a información que de otra manera se mantiene oculta. Tengamos en cuenta que el verdadero hacker ha llegado a tener cierto poder en sus manos. Sin embargo esa faceta romántica permitió que actuaran de buena fe y se comportaran como caballeros. Una vez que uno tiene poder es mucho mejor abstenerse de usarlo que usarlo mal”.

“Normalmente hay etapas en la vida de toda la gente donde tiene más o menos dedicación a una actividad. Hay muchos hackers que se aíslan de la realidad, lo cual puede ser válido o no. Se puede establecer un perfil, en general es una persona con profundos conocimientos técnicos, es un poco un nuevo marginado, un nuevo bohemio, un nuevo artista”.

“Hoy en día el hacker ya se fue incorporando al tejido de la sociedad, podemos encontrar hackers de todo tipo. Es difícil definir un perfil único de hacker. Podemos encontrar hackers de derecha, de izquierda, sin ideología política, homosexuales, lo que quieran”.

“En general el hacker se inicia durante la adolescencia porque en ese momento tiene la capacidad intelectual para dedicarse al tema y dispone del tiempo”.

"Captain Zap", se consagró como hacker a los veintitrés años cuando

ingresó ilegalmente vía módem a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

También violó los accesos restringidos a compañías electrónicas para tener acceso a órdenes de mercancías, archivos y documentos del gobierno.

A los dieciséis años se hizo famoso al irrumpir en los servidores de la

Nasa, siendo condenado a seis meses de cárcel en una prisión juvenil.

“Es el poder en la punta de tus dedos. Puedes controlar todas estas computadoras, desde las del gobierno, las militares y la de las grandes corporaciones. Es un viaje de poder.

Los sitios desprotegidos no me llaman la atención. Yo apuntaba a un lugar porque significaba un gran reto.

Yo no cubrí todas las pistas del todo, y si lo hubiese hecho, ellos jamás habrían tenido la capacidad de capturarme.

Podría haber borrado archivos, o colocar un virus o vender la información a países extranjeros. Podría haber ejecutado una negación del servicio y causar que las redes de computadores queden fuera de funcionamiento. Alguien podría haber realizado una enorme cantidad de cosas que yo no hice.

Le llaman daños cuando un entusiasta de las computadoras, como yo, les demuestra su ineptitud”.

Algunos estudios muestran que las características más comunes de personalidad en hackers son su alto nivel intelectual, gran curiosidad y facilidad para abstracciones. Aunque una alta inteligencia en general es común entre hackers, existe otra característica que considero más importante: la habilidad mental de absorber, retener, y referenciar grandes cantidades de detalles aparentemente sin importancia basados en la experiencia que le dan contexto y significado. Deben recordar y aplicar lo que está escrito en numerosos manuales de software.

Son extraños en lo que se refiere al control y orden. Ellos tienden a tener el control absoluto de un sistema modificándolo a su propio gusto. Cuando más control tengan de un sistema, más interés le atribuyen para poder mantenerlo siempre a un nivel de eficiencia. Para todo esto se necesita orden. Los hackers son intelectualmente ordenados. Muy meticulosos con lo que dicen o hacen.

Siguiendo a Liberman podrían presentar un estilo reflexivo con un subestilo dramático con suspenso. Este estilo reflexivo las muestra como personas agudamente observadoras, con un predominio de lo racional. El hacking para ellos consiste en una actividad meramente vouyerística e intelectual. Pueden presentar rasgos épicos cuando lo utilizan con afán reivindicativo, o justiciero; o bien con rasgos histriónicos que son los que generalmente relatan sus hazañas para reforzar su autoestima.

Son generalmente buenos escuchas y más bien pasivos. Disociados. Su ideal del yo es muy alto, así como su conciencia y su moral.

Tienden a manejarse ingenuamente y se mueven con la lógica y por lo general no comprenden aquello que no siga esa lógica. Necesitan estar solos y disfrutan de esa soledad.

Toman distancia y necesitan de ella para funcionar bien. Discriminan lo fundamental de lo accesorio con facilidad, y funcionan bien en las actividades autónomas; no les gustan los horarios fijos ni el control externo.

Es su necesidad de autoexcluirse emocionalmente constantemente, es él quien excluye al otro, lo único que puede hacer es observarlo sin participar. Tener permanentes sospechas (incógnitas) acerca de las demás personas a quienes observa y estudia omniscientemente como “bichos raros”.

Les cuesta expresar los afectos. Tienen miedo a la agresión, evitan los conflictos pero se mueven en términos de blanco o negro. Se desempeñan muy bien en tareas que deban realizarse individualmente, utilizando la capacidad de abstracción.

Requieren una posición para mirar desde lejos, rechazan la invasión, pero son muy dependientes a pesar de parecer desapegados.

La estructura esquizoide lleva implícita la dificultad en participar (dar), sumada a una urgencia voraz por observar (tomar, conocer e incorporar).

Cuando fallan sus mecanismos defensivos pueden mostrarse con un subestilo dramático con suspenso. Esto se relaciona con la estructura fóbica.

El control que intentan ejercer, mostrándose alertas, está al servicio de sentirse a salvo. Necesitan mantener con el otro una “distancia óptima”, ni demasiado cerca como para vivirlo como un peligro, ni demasiado lejos como para sentirse no tenidos en cuenta. Se percibe una cierta sensación ansiosa en ellos.

Tienen mucha necesidad de afecto pero al mismo tiempo, necesidad de moverse sin que lo encierren. Presentan problemas en todo lo relacionado con la angustia. En su vida diaria son independientes y funcionan en tareas autónomas y con movilidad. Esta movilidad les permite ser muy creativos y no se adaptan a las rutinas.

Son personas con mucha independencia, que encubre su dificultad para establecer vínculos, por su temor a quedar encerrados y sin aire. Así, su agresión se convierte en ansiedad e impulso a la fuga.

Un hacker en general no se motiva con premios convencionales tales como la aprobación social o el dinero. La motivación última del hacker es de índole intelectual, es un reto personal en el que intenta ponerse a prueba a sí mismo intentando saltar las medidas de seguridad de sistemas cada vez más complicados, aprendiendo así un poco más día a día.

Dentro de las comunidades hacker, se da más importancia a la persona que ha obtenido sus conocimientos de manera autodidacta, ya que se la considera mejor motivada que la que se adapta a la obligatoriedad de una escuela.

Las áreas académicas de mayor tendencia entre hackers son ciencias de la computación, ingeniería, física y matemáticas.

Los hackers jamás *trabajan* bajo su verdadero nombre, sino que emplean pseudónimos para enmascarar su verdadera identidad como si fuesen superhéroes. Podría tratarse de sujetos algo elitistas, pero no se trata de introvertidos sin vida social. Puede que salgan poco, pero se comunican bastante por Internet, y por supuesto tienen conciencia de comunidad, aunque ésta sea virtual.

De hecho, el grupo de pares de un hacker es muy importante para ellos, dado que sus hazañas y logros para que sean experimentados como tales, deben pasar por la opinión grupal, quienes lo llaman hacker o no. Es decir, un sujeto nunca se autodenomina hacker, sólo será un verdadero hacker cuando así lo decida su comunidad.

Quizá el único posicionamiento ideológico reside en admitir que la información debería ser universal (de libre acceso), y a la vez hacer cualquier cosa para acceder a esta información. De este modo, ellos reconocen que la información es en sí misma un valor, pero no reconocen que este valor pueda ser propiedad privada.

Si no fuera por esta pequeña contradicción, el perfil del hacker no sería distinto del de cualquier adolescente obsesionado con su afición, ya sea ésta el motociclismo, el violín o el fútbol. Un grupo de iguales con los que conversar del tema, unos acontecimientos clave, y otra vez a reunirse para seguir rememorando el episodio.

Generalmente esta pasión por los ordenadores continúa cuando se deja atrás la adolescencia. Se puede profesionalizar, se puede canalizar, pero queda para siempre como una gran afición. Generalmente después de la adolescencia, trabajan dando consultorías informáticas o en empresas de seguridad en software.

Considero que este perfil presenta un grado de peligrosidad relativamente bajo, ya que en general son sujetos que respetan y comparten un estricto código ético, y dado que el dinero no es una motivación para ellos en el uso de computadoras, sólo les interesa lograr acceder a lugares que ellos se proponen; no aceptarían ser pagados para llevar a cabo una acción de índole delictiva.

Por su parte, un phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también saben sobre el funcionamiento de las tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

En general construyen equipos electrónicos artesanales para interceptar, y hasta ejecutar, llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

Estos sujetos buscan burlar la protección de las redes públicas y corporativas de telefonía con el declarado fin de poner a prueba conocimientos y habilidades -en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación-, pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores.

Los phreakers tienen un único objetivo: las empresas telefónicas. Poseen conocimientos para derivar la factura a alguna multinacional.

Difícilmente un phreaker querrá hacerse rico a base de estafar a una empresa de servicios telefónicos. Lo que sucede es que considera que la compañía estafa a todo el mundo y “quien roba a un ladrón, tiene cien años de perdón”.

Sobre este perfil se muestran los siguientes fragmentos:

Dark Dante: llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada era la ciento dos.

Cóndor: fue capaz de crear números telefónicos imposibles de facturar, tenía el control de tres oficinas centrales de teléfonos en Manhattan y de todos los centros de conmutación de California, dándole la posibilidad de escuchar cualquier conversación telefónica o, si no eras una persona de su agrado, modificar el teléfono de tu casa de tal manera que, cada vez que levantaras el auricular, una grabadora pedía que depositaras 25 centavos.

En cuanto a su estilo comunicacional, considero que lo comparte con el perfil hacker, es decir, es también un estilo reflexivo (esquizoide), con un subestilo dramático con suspenso (fóbico).

Este grupo a diferencia del anterior posee una motivación extrínseca porque lo que persiguen es no tener que pagar una factura, y esto se traduce en dinero.

Por lo demás, se parecen bastante a los crackers y no tienen, desde luego, la ética del hacker.

Su grado de peligrosidad es mayor que la del hacker porque pueden controlar los sistemas de telefonía –escuchas telefónicas-, y si tienen un objetivo o intención detrás de esto, pueden usarlo como una herramienta para cometer un delito.

**6.3.2 - Psicología Cracker y Virucker**

El término crack en inglés significa rotura y por lo tanto implica provocar daños tanto en la programación de software como del hardware. Así es fácil comprender que un cracker debe conocer perfectamente las dos caras de la tecnología informática, esto es la parte de programación y la parte física de la electrónica.

Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutada automáticamente puedan vulnerar claves de accesos de los sistemas ubicados en cualquier parte del mundo.

Los miembros de este grupo no tienen habilidades significativas en programación, no conocen términos extremadamente técnicos, ni tampoco tienen experiencia en plataformas Unix u otros sistemas multiusuarios.

Sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware –programas de distribución gratuita- para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anticopia.

Entre las variantes de crackers maliciosos están los que realizan *Carding* (tarjeteo, uso ilegal de tarjetas de crédito), o *Trashing* (basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos).

De los casos seleccionados tenemos los siguientes crackers:

Shadowhack tenía dieciséis años cuando violó el acceso a la empresa

telefónica AT&T y los sistemas del Departamento de Defensa de EE.UU. Fue sentenciado por la destrucción de archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publicó contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales.

“X-Team" fue el primer grupo de piratas informáticos argentino dedicado

a las intrusiones de carácter político; irrumpieron en la página web de la Corte Suprema de Justicia Argentina, cambiando su portal, y reclamando la solución urgente del crimen del periodista José Luis Cabezas.

El Cóndor: fue sospechoso de robar el software de más de media docena

de fabricantes de teléfonos celulares de los EE.UU.

Las organizaciones susceptibles de ser atacadas por un cracker tienen que proyectar una imagen pública que resulte odiosa para cualquier joven anti-sistema: bancos, medios de comunicación, gobiernos, grandes empresas que estén en boca de la opinión pública por actividades “contra el pueblo”

La satisfacción se obtiene en este caso por sabotear sistemas, por dañar a una organización. Tienden a agruparse en grupos pequeños, muy secretos y privados. También se los ha llamado *cyberpunks*, sobre todo por la filosofía anti-sistema y porque muchas veces sabotean sistemas informáticos de grandes empresas que acumulan cuantiosos beneficios.

A diferencia del hacker que tiene como intención observar sin participar, curiosear sistemas informáticos ajenos, a los que accede ilegalmente pero que no modifica, generalmente el cracker tiene como intención intrínseca, destruir. También puede actuar de acuerdo con una motivación extrínseca: entrar en un sistema para sustraer información, hacer copias y venderlas a un módico precio, es una práctica habitual y es el fraude más extendido en el mundo de la informática.

Podría pensarse que son personalidades con un estilo reflexivo y que se manejan con un subestilo épico.

El estilo de acción o épico se relaciona con la estructura psicopática. Estas personas generalmente tienen reglas propias y dividen para imperar. No toleran los límites, ni los tienen; su mayor éxito es que no sepan como son ni donde están. Toman y abandonan episódicamente las parejas, los trabajos y cualquier cosa estable.

Su característica principal es el aburrimiento y el tedio.

Su trastorno de la capacidad de pensar con símbolos verbales acerca de las cosas que necesitan, da lugar a la manera típica de reaccionar ante una frustración y una forma particular de experimentar angustia, sienten tensión y depresión y sufren tedio o hastío.

Tienen pensamiento concreto y actitudes en última instancia autodestructivas.

Experimentan alivio con una actuación psicopática. En ellos aparece la necesidad de hacer algo, pero sin saber qué, acompañado todo esto de un malestar que les provoca tensión, malhumor e irritabilidad a todo tipo de estímulos.

Las personas con estas características poseen una modalidad de comportamiento específica y muchas veces no presentan síntomas manifiestos. En su comportamiento no muestran indicios que indiquen una forma asocial y solamente su conducta pasada futura mostrará la más destructiva de todas las formas conocidas.

No tienen sentimientos de culpa y su aparente temor es más bien paranoide. Producen fascinación en los oyentes y una suerte de impacto que hace que en poco tiempo se sienta que se los conoce de toda la vida.

Poseen una ética propia y tratan a los demás como su superyo los trata a ellos.

Las personalidades psicopáticas buscan consumar con un tercero un acto de venganza -que ellos consideran justiciero- por las injurias narcisísticas sufridas en el curso de la vida, en especial en la temprana infancia.

Utilizan la inoculación, con mensajes que constituyen una orden en el receptor (actuación). De esa manera el emisor procura apoderarse de la voluntad del receptor para sacar un beneficio en detrimento de éste.

Al no poseer sentimientos de culpa, y manejarse con una ética y límites propios este perfil presenta un grado de peligrosidad elevado y podrían ser muy capaces de cometer delitos de guante virtual.

Por otra parte, el grupo del perfil virucker tiene por objetivo el ingreso doloso a un sistema informático ajeno, para introducir "virus" o “gusanos” y destruir, alterar y/o inutilizar la información contenida.

Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

Los siguientes fragmentos ilustran este perfil:

Smith, David. Un programador detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa".

El impacto de Melissa había afectado de forma sustancial a los buzones virtuales de correo de una gran parte de sus catorce millones de usuarios.

Fue precisamente el modo de actuar de Melissa, que remite a los cincuenta primeros inscriptos en la agenda de direcciones del cliente de correo electrónico "Outlook Express", centenares de documentos "Office” fueron la clave para encontrar al autor del virus.

Los ingenieros informáticos rastrearon los primeros documentos que fueron emitidos por el creador del virus, buscando encontrar los signos de identidad que incorporan todos los documentos del programa de Microsoft "Office" y que en más de una ocasión han despertado la alarma de organizaciones en defensa de la privacidad de los usuarios.

Una vez desmontado el puzzle de los documentos y encontradas las claves se consiguió localizar al creador del virus Melissa. Sin embargo, la detención de Smith no significó que el virus hubiera dejado de actuar.

Robert Morris lanzó un programa "gusano" diseñado por él mismo para navegar

en Internet, buscando debilidades en sistemas de seguridad, que pudiera correrse y multiplicarse por sí solo.

Eliminar al gusano de sus computadoras causó a las víctimas muchos días de inactividad y millones de dólares de pérdida.

Por sus características psicopáticas podría suponerse a este grupo cercano en su dinámica psíquica con el estilo comunicacional cracker, ya descrito, es decir, reflexivo con un subestilo épico. El grado de peligrosidad de este grupo que se dedica a infectar y enfermar sistemas con virus es considerablemente peligroso y el más difundido por el ciberespacio.

No poseen conciencia de comunidad, actúan individualmente y no se rigen por ningún código ético, son al igual que los crackers, anarquistas.

**PARTE III - CONCLUSIONES**

En esta etapa de la cultura posmoderna, que es parte del fenómeno de la globalización, el mundo virtual del ciberespacio propicia un anonimato en la red Internet que comienza a tener implicancias jurídicas cuando se usa a través de diversas técnicas con fines delictivos.

Tal como fue considerado en el marco teórico, generalmente la delincuencia informática responde a conductas que no se realizan en un solo acto, sino en una serie continuada de ellos, y los daños pueden ser experimentados por individuos o grupos -bancos, empresas, instituciones- en un país distinto a aquel donde se encuentra el delincuente físicamente.

Una vez producidos, es posible eliminar toda evidencia de su realización, lo que produce dificultades para el descubrimiento y la prueba; y con frecuencia su ilegalidad no es clara, es más, depende el país donde el delito se emita.

Generalmente, el problema se presentó en que el imaginario social popular, trata a los delitos informáticos como si fueran realizados por hackers, pero los estilos de personalidad son diferentes según el objetivo o la intención con la que se utilicen las técnicas de hacking en el ciberespacio.

Se observó que en los últimos cuarenta años, se fueron formando grupos de comunidades virtuales en el ciberespacio que contenían una filosofía y una ética propia, a partir de los casos seleccionados de ataques a organizaciones y empresas provenientes del exterior de la misma, se delinearon cuatro perfiles de personalidad según su actividad en la red.

Así, tanto *hackers,* -sujetos hábiles en violar la seguridad de los sistemas informáticos- como *phreakers* –sujetos hábiles en violar los sistemas telefónicos- poseen un estilo comunicacional reflexivo, -relacionado con las esquizoidías-, y un subestilo de tipo dramático con suspenso (fóbico) y rasgos épicos, si bien no poseen la intención de dañar la información, sino de curiosear y llegar más allá de los límites impuestos. La motivación última del hacker es de índole intelectual, mientras que la del phreaker es evitar pagar un servicio y burlarse, teniendo el control de los sistemas de telefonía.

En cuanto a los *crackers* –sujetos hábiles en violar y destruir software y hardware- y a los *viruckers* –sujetos hábiles en la propagación de gusanos y virus– podría pensarse que presentan un estilo comunicacional también reflexivo, con un subestilo épico o de acción, relacionado a las psicopatías, dado que ambos comparten la intención de causar daño en sus ataques, aumentando también su grado de peligrosidad.

Estos perfiles pueden presentarse juntos en un mismo individuo o separados.

En cuanto a su tratamiento psicológico, es difícil que estos sujetos concurran por sí mismos a terapia, ya que desconfían de alguien que pueda comprender su propia dinámica psíquica -sería para ellos que les invadan su software- y por sus características de personalidad tienen una alta resistencia a ello, ya que consideran que se sienten controlados y analizados.

En caso de que lleguen a tratamiento por derivación considero que el psicólogo tendría que posicionarse desde un estilo complementario, poético -relacionado con la histeria- para poder ayudarlo a integrar el pensamiento, la conducta y la emoción.

En síntesis en esta investigación he tratado de aportar elementos de juicio interdisciplinario:

Para la Criminología: el dar a conocer una novedosa modalidad delictiva y a través de ello,

Para el Derecho: resaltar las lagunas al respecto en nuestro Código Penal,

Para la Psicología: plantearse cómo tratar a este tipo de sujetos y proponer el análisis sistemático de los diversos perfiles de personalidad para prevenir a todos los sectores de la sociedad sobre su alcance, y propiciar que se formalice la psicología ciberforense como una rama especializada que se active a medida que avance la tecnología informática, incorporando elementos humanos sobre lo técnico que presenten características delictivas ocultas dentro de la virtualidad del ciberespacio.

Desde una perspectiva personal, considero que un sistema siempre va a tener fallas por su naturaleza, pero a qué velocidad y cómo se resuelvan estas fallas podrían depender las posibilidades de cometer delitos de guante virtual en el ciberespacio.

**ANEXO I**

**GLOSARIO DE TÉRMINOS**

**Acceder, acceso:** Define la acción de entrar, visualizar o consultar una página o dirección en Internet. También la cantidad de veces que una página es consultada. Una página que no es conocida no puede ser visitada y por lo tanto las posibilidades de negocio a través de la misma son menores. Las actividades de promoción en Internet van encaminadas a facilitar el conocimiento de la dirección de una página y unos contenidos atractivos para que los clientes tengan interés en visitarla regularmente. Para el comercio de e-books es imprescindible tener los productos en lugares que permitan el conocimiento de los mismos.

**Acceso root.** Entrar en un sistema con el usuario root.

**Administrador.** Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total, sin restricciones.

**ADSL:** Asymmetric Digital Subscriber Line. Estas son las siglas de la tecnología que permite una conexión permanente de gran velocidad para poder transmitir datos y voz al mismo tiempo. Cada vez se usa más tanto por empresas como por particulares, lo cual facilitará la transmisión y el acceso a través de Internet a documentos o datos de mayor tamaño en menor tiempo.

**Ancho de banda (bandwidth) :**Define la cantidad de datos que pueden ser transmitidos por una red en un determinado tiempo, normalmente bites por segundo.

**Archivo adjunto, attachment**: Es todo archivo que acompaña a un correo electrónico. Suele representarse como un clip unido al mismo.

**Antivirus:** Programa que encargado de evitar que cualquier tipo de virus entre a la computadora y se ejecute. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

**Ataque:** Define especialmente la acción contra una web, página web, proveedor o empresa que pueden realizar los hackers. Mediante esta acción, pretenden entrar en las páginas públicas o privadas para tomar control de las mismas y realizar acciones como toma de datos, destrucción o simplemente cambios. Las compañías desarrollan sistemas de seguridad para evitar la entrada de personas no autorizadas en las mismas. Acciones de ataque pueden ralentizar y hasta colapsar servicios en Internet.

**Autenticación:** Mediante esta acción se requiere al usuario que introduzca su nombre y contraseña a fin de comprobar que tiene autorización para acceder a determinada información. El acceso controlado permite ofrecer servicios sin límites a usuarios registrados, sin que ello signifique un trabajo adicional para quienes los suministran, ya que el sistema gestiona automáticamente el acceso y la difusión de la información.

**Backdoor.** Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal.

**Bajar, descargar, copiar, download:** Es la acción mediante la cual un usuario en Internet descarga en un ordenador un fichero que estaba situado en un servidor de la red. Estos ficheros pueden ser textos, imágenes, sonidos, o todo a la vez. Los e-books son bajados desde el servidor hasta el ordenador o dispositivo donde se colocan para su lectura.

**Banner:** Define el objeto o lugar dentro de una web donde se coloca cierta información con un fin promocional. Los banners son una invitación a los usuarios para introducirles en otra página, donde pueden obtener más información acerca del tema sobre el cual les informa el banner.

**Black Box:** Aparato que engaña a la central telefónica haciéndole creer que no se levantó el tubo del teléfono cuando en realidad se está produciendo una comunicación.

**Bombas ANSI**: Utilizando los códigos ANSI, se asigna una acción destructiva a alguna tecla. Me explico, ANSI es un conjunto de códigos estándar. Si en tu computadora uno de estos códigos lo ejecutara. Los códigos ANSI se usan para varias cosas, entre ellas, cambiar los colores de la pantalla, posicionar el cursos, y el método que usan las bombas ANSI, asignar a una tecla una acción determinada. Si esta acción es dañina al pulsarla hará el daño.

**Bomba lógica o cronológica:** Programa que tiene como función la destrucción o modificación de datos en un tiempo determinado. Al revés de los virus o los gusanos, las bombas lógicas son las que poseen el máximo de potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un recate a cambio de dar a conocer el lugar donde se halla la bomba.

**BPS:** Se refiere a la velocidad con la que se transfieren datos en Internet. El término es bits por segundo.

**Browser, explorador, navegador, visualizador:** Este término se refiere a los programas que facilitan el acceso y recorrido por las distintas webs o páginas que hay en Internet. Los más famosos son NAVIGATOR de Netscape, y EXPLORER de Microsoft.

**Bug:** Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

**Buscador, motor de búsqueda:** Son los lugaresen Internet que ofrecen la posibilidad de realizar consultas sobre una base de datos donde ellos tienen clasificados distintos sitios de Internet en razón de la materia que contienen. Hay una enorme cantidad de buscadores que permiten consultar por textos o palabras claves, muchos de ellos especializados en materias concretas o en un determinado lenguaje; sin embargo hay otros que son multiculturales y multilenguaje como Yahoo, Altavista, Lycos o Infoseek.

**Caballos de Troya.** Es un programa que aparenta ser otro programa y además de hacer lo que realiza este, realiza acciones no deseadas (como borrar archivos).

Un troyano común en UNIX es un SU que al pedirnos la clave la almacena en un lugar, y nos hace creer que la hemos introducido mal (caso muy frecuente), en este momento el troyano se borra a sí mismo y la siguiente vez que se ejecute él SU se ejecutara él SU verdadero, con  lo que el usuario no se dará cuenta, mientras que su clave queda almacenada para poder ser usada mas tarde. Otro troyano típico es un programa que nos pide que se ejecute con privilegios de supervisor, y cuando lo ejecutamos además de hacer su trabajo se dedica al borrar todo lo que puede.

**CERT.** Es un equipo de seguridad para la coordinación de emergencias en redes telemáticas.

**Certificación:** Mediante este procedimiento una entidad o sistema garantiza la identidad de la organización o persona que emite un dato o requiere ser conocida. Normalmente se utiliza para confirmar que un determinado programa, contenido o la firma electrónica pertenece a dicha persona u organización.

**Cifrar, descifrar, encriptar, descriptar, desencriptar:** Es el proceso criptográfico mediante el cual se oculta una información utilizando números en vez de letras a través de una clave. Esta tecnología es la que se usa para la creación de determinados E-books protegidos para evitar su copia. Mediante el descifrado se accede a la información tal como estaba antes de la protección.

**Clave, clave pública:** La clave es la llave que permite encriptar o desencriptar una información. La clave pública es una contraseña que un usuario puede usar conjuntamente con una clave privada; la pública puede ser enviada a otros para cifrar un mensaje y la privada es la que le permite a ese usuario descifrar el mensaje que le ha sido remitido mediante su clave pública.

**Clic, picar, pinchar:** Es la acción mediante la cual se selecciona un objeto o texto, que aparece en la pantalla, y que se encuentra vinculado a otro, ya sea objeto, información o lugar, a través de un enlace.

**Contenido:** Este concepto se refiere a la información contenida en un sitio de Internet. También a la información que incluye un fichero de datos alojado en la misma o a la que se transfiere, carga o descarga en la red. El contenido es fundamental para captar la atención de los navegantes, y por ello, las empresas que desarrollan comercio en Internet ofrecen contenidos atractivos para conseguir que los clientes acudan a su web.

**Contraseña:** Mediante la contraseña se controla el acceso a determinadas páginas o contenidos en Internet. También se utiliza para la producción de páginas exclusivas que se crean automáticamente según el perfil del usuario que accede a ellas. Esto es muy interesante, pues permite ofrecer productos o servicios específicos según los interesantes preestablecidos del consumidor.

**Cookie:** Se refiere a un pequeño archivo que es enviado desde la web que es visitada hasta el ordenador de la persona que la consulta. Este archivo queda almacenado en el disco duro del usuario y permitirá identificarle cuando vuelva a visitar esa misma web. Este método facilita que el sistema pueda configurarse automáticamente para ofrecer, por ejemplo, productos o servicios que dicho usuario haya consultado en la anterior visita.

Es un pequeño trozo de información enviado por un servidor de Web al buscador de un usuario. Cuando se visita un servidor que utiliza el desarrollo denominado “Magic Cookie (MC)”, éste instruye al buscador de la PC para crear un archivo Magic Cookie al que se lo suele nombrar como cookies.txt o similar. En él, ingresa y queda una pequeña cantidad de información, dicho bloque de datos podría contener un identificador exclusivo para el usuario generado por el servidor, la fecha y hora actual, la dirección IP del proveedor del servicio de acceso a Internet mediante el cual la PC del usuario se conecta a la red, o cualquier otro grupo de datos que se desee.

**Correo electrónico, e-mail:** Es el medio por el cual se intercambian mensajes en Internet a través de programas específicos para su gestión.

**Cortafuegos (Firewall):** Mediante estos programas se impide el acceso a personas no autorizadas a un ordenador o red. Con estos dispositivos se pretende mantener seguros los contenidos que se encuentran alojados en un sistema y son fundamentales para evitar la piratería informática. En el caso de los e-books los contenidos ofrecidos para su descarga se encuentran protegidos previamente mediante la encriptación.

Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red de área local (LAN) de una organización en Internet. La barrera de protección impide que los crackers tengan acceso a la red interna. Por desgracia, también impide que los usuarios de la organización obtengan un acceso directo a Internet. El acceso que proporciona la barrera de protección es indirecto y mediado por los programas llamados servidores apoderados.

**Cracker:** Persona que quita la protección a programas con sistemas anticopia;   
y que se dedica a destruir información.

**Criptografía:** Criptografía proviene del griego y se puede traducir como “La manera de escribir raro” (criptos de extraño y graphos de escritura). Consiste en modificar los datos de un archivo o los que se transmiten por módem, radio, etc. Para evitar así que los puedan leer personas no deseadas. Esta técnica ha tenido su principal aplicación en los ejércitos y en la diplomacia.

**Cyberpunk:** Corriente literaria dentro de la ciencia ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

**Dirección, localizador, URL:** Define el lugar donde se encuentra una web o un contenido específico en Internet. Esta es la información que se difunde públicamente en Internet a través de los distintos servidores que la componen, para que cualquier usuario pueda acceder a la misma. Los navegadores la utilizan para localizar el lugar a donde quiera llegar el usuario. Aunque normalmente usamos unas palabras precedidas de “**http.//www.”** , los sitios en Internet se encuentran definidos por una secuencia numérica que define el país y el proveedor de la información mediante un registro de carácter mundial.

**Dominio:** Mediante ellos se concretan los lugares de Internet donde se encuentra alojada una información. Indefectiblemente un dominio se encuentra unido a una URL para poder ser localizado en Internet. Existen dominios de alto nivel como los que definen los países “.es”, y de primer o segundo nivel cuando se incorporan distintas palabras precedidas de un punto a estos dominios de alto nivel.

**E-book:** Es una publicación que ha sido confeccionada digitalmente para poder ser comercializada en Internet. Su diseño, estructura y tamaño han tenido que ser tratados correctamente para que su visualización, tiempo de transmisión y posibilidades de utilización sean los adecuados para responder a las necesidades y aprovechar las posibilidades de servicios adicionales que ofrecen las publicaciones digitales a través del comercio electrónico. Con objeto de proteger los derechos de los autores y editores, así como garantizar el comercio de los e-books, se han desarrollado sistemas que posibilitan la protección de los contenidos para evitar su copia e impresión sin la autorización de los propietarios. Estos sistemas también garantizan a los consumidores que ellos han adquirido un producto determinado con unos derechos para su uso.

Las empresas que proporcionan estos servicios usan fundamentalmente dos tipos de soluciones para la creación y protección de los e-books: uno basado en el Adobe Acrobat Ebook Reader y el otro en el Microsoft Reader. Por otro lado también se denominan e-book a los propios dispositivos portátiles en los que se pueden cargar los e-books para ser consultados.

**E-bussiness, E-commerce:** Definen los negocios o acciones comerciales que se desarrollan a través de Internet. Desarrollar un método para el comercio de e-book conlleva ineludiblemente la necesidad de buscar un sistema para el comercio electrónico (e-commerce) y preparar una estrategia de negocio específica para este entorno (e-bussiness). La ayuda de unos especialistas es imprescindible para el enfoque adecuado y las acciones precisas que permitan aprovechar todas las oportunidades que ofrece Internet.

**Enlace, link, vínculo, hipervínculo:** Consiste en una imagen o texto destacado, mediante subrayado o color, a través del cual se puede acceder a otro sector del documento o a otra página web, con el que se encuentra conectado, con sólo pulsar sobre él.

**Falsificación de software.** La falsificación de software ocurre cuando un programa es ilegalmente duplicado y luego vendido como si se tratara de un producto legitimo. Los falsificadores pueden copiar el producto completo, incluyendo documentación, discos, etiquetas y hasta elementos de seguridad como hologramas.

**Firma electrónica:** Mediante este proceso el autor de un documento certifica que es suyo. Para el reconocimiento de la misma es necesaria que dicha firma sea certificada por una autoridad competente. Existen en estos momentos diversas iniciativas para el reconocimiento de las firmas electrónicas, entre las que se encuentra la propia Administración Pública española.

La firma electrónica será muy importante en el futuro para todo tipo de transacciones electrónicas y podrán permitir, una vez registrado y reconocido el cliente, que los sistemas de pagos puedan ser distintos a los habituales en estos momentos.

**FTP.** (File Transfer Protocol: Protocolo de transferencias de archivos) Un conjunto de protocolos mediante el cual pueden transferirse archivos de una computadora a otra. FTP es también el nombre de un programa que usa los protocolos para transferir archivos de ida y vuelta entre computadoras.

**Guest o Invitado.** Cuenta pública en un sistema, para que la use alguien que no tiene una cuenta propia.

**Gusanos.** Son programas que se transmiten a sí mismos de una maquina a otra  a través de una red. Se fabrican de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras el virus es un tumor maligno.

Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

**Hacker.** Persona que se introduce en un sistema sin tener autorización.

**Handle.** Seudónimo usado en lugar del nombre verdadero.

**Hardware.** Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

**Hit, impacto, visita:** Se denomina así a la cantidad de veces que la página web es visitada por los usuarios. El número de acceso está en relación con el éxito que esa web y, como consecuencia, los servicios ofrecidos están obteniendo. Desarrollar sistemas que faciliten el conocimiento y las visitas son fundamentales para el comercio electrónico.

**HTML:** *Hyper Text Mark-Up Language.* Es el lenguaje básico de programación en Internet. Mediante él se crean las páginas webs para que puedan ser visibles desde cualquier tipo de sistema informático.

**http:** Esta abreviatura define el protocolo de transferencia de hipertextos. Este es un protocolo que permite traspasar información en archivos de texto, gráficos, de video, de audio, y otros recursos multimedia.

**Ingeniería social.** Arte de convencer a la gente de entregar información que no corresponde.

**Internet.** Sistema de redes de computación ligadas entre si, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

**ISP:** *Internet Service Provider.* Proveedor de servicios de Internet; es la compañía que ofrece la conexión a Internet, e-mails y otros servicios relacionados, tales como el diseño y el almacenaje de páginas web.

**Key logger.** Grabador de teclas pulsadas. Se utiliza para cuando deseamos saber las contraseñas, este programa graba cuando el usuario ingresa su contraseña. También se utiliza para saber cuales han sido las acciones de los usuarios en el sistema.

**Lamer:** Tonto, persona con pocos conocimientos o con poca "NET-iqueta".

**Login, Username, Usuario.** Nombre de registro de entrada. En una red de computación, nombre único asignado por el administrador del sistema usuario, que se usa como medio de identificación inicial. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

**Mb, meganyte; Gb gigabyte:** Son unidades de medida en informática. Los Mb, o simplemente los bytes, miden el tamaño de ficheros, discos duros o cualquier tipo de unidades de almacenamiento. El tamaño es un elemento fundamental en Internet; la transmisión de datos se mide según la velocidad con la que son transferidos en segundos.

**Microsoft Reader:** Es el software desarrollo por Microsoft para la creación y visualización de e-books protegidos.

**Operador:** Persona que usa una computadora. A menudo se llama "operador" al administrador del sistema.

**Pasarela, gateway:** Es un dispositivo o protocolo mediante el cual se conectan dos redes o servidores para realizar algún tipo de transacciones especiales. En relación con el comercio electrónico, son habituales las pasarelas de pago directas con el banco, mediante las cuales los consumidores realizan el pago directamente a una entidad bancaria aunque la compra la estén haciendo en un sistema de comercio electrónico. La web donde se realiza la compra se conecta mediante una pasarela de pago al banco para que el consumidor realice la transacción, mediante tarjeta de crédito, directamente con el banco.

**Password, Contraseña.** Es una herramienta de seguridad empleada para identificar a los usuarios autorizados de un programa o de una red y para determinar sus privilegios, como el de solo lectura, el de lectura escritura, o el de copiado de archivos.

**Match:** En inglés, parche. Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

**Payload:** Efecto visible de un software maligno.

**Pirateria de software:** Copia ilegal de software con derecho de autor sin que medie el permiso expreso del editor.

**PDF:** *Portable Document Format.* La mayoría de los programas informáticos para la composición de textos y la maquetacion pueden convertir sus ficheros a PDF. Una vez convertido, cualquiera puede abrir el documento usando una gran variedad de harware y software, manteniendo exactamente la presentación, las fuentes, los vínculos y las imágenes del fichero original. Usando Adobe Acrobat se genera, en formato PDF, un fichero digital exactamente igual a la presentación de los libros en formato papel.

**Pesar:** Define el tamaño en Mb que tiene un fichero; el peso tiene una incidencia directa sobre el tiempo de transmisión y por supuesto, en los costes para su almacenamiento y comercio. El diseño de los e-books tiene que conseguir que su peso o tamaño sea el adecuado para que el tiempo de descarga por el consumidor sea el menor posible.

**Portal:** Define un lugar en Internet donde los usuarios pueden acceder a una serie de servicios. Existen portales generales, donde los usuarios pueden encontrar información de todo tipo, y portales verticales que están desarrollados para ofrecer información muy especializada sobre una temática concreta. Los portales son unos lugares muy interesantes para captar clientes, ya que ofrecen la posibilidad de colocar publicidad. Sin embargo, parece que la efectividad de los banners es mucho mayor en portales verticales que en portales generales.

**Rabbit:** En inglés, conejo. Programa que provoca procesos inútiles y se reproduce (como los conejos) hasta que agota la capacidad de la máquina.

**RDSI, ISDN:** Es el sistema de transmisión de datos o voz por teléfono, con una capacidad mayor a la de la red normal, no solo en cuanto a la velocidad de transmisión sino también por la posibilidad de usar dos canales de comunicación al mismo tiempo.

**Redirigir:** Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

**Root:** Cuenta del administrador en UNIX. Es la más poderosa: permite el acceso a todo el sistema.

**SATAN.** El SATAN, Herramienta para el Análisis de Administradores de Seguridad de Redes  (Security Administrator Tool for Analyzing Networks) es una aplicación realizada por el informático norteamericano Dan Farmer y el gurú cibernético americano-holandés Wietse Venema. Esta es capaz de adivinar el nivel de vulnerabilidad de un host (ordenador servidor de Internet) y de todas las máquinas conectadas a él vía Internet (su dominio), ya que permite conocer su nivel de encriptación, password, etc. SATAN también se puede obtener libremente por FTP en la red, lo que significa que puede ser utilizado tanto por los propios servidores para ver su nivel de vulnerabilidad como por los hackers. Es por tanto un arma de doble filo.

**Servidor, Server:** Define el equipo que hace las funciones de almacenaje y entrega de las peticiones que la realizan los usuarios o clientes. La potencia de los servidores es fundamental para que puedan procesar las órdenes y servirlas en un tiempo adecuado.

**Shell:** Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del sistema operativo las ejecute.

**Shoulder Surfing:** Espiar por detrás de un hombro para tratar de ver información interesante. Al cual estamos muy expuestos, y es un método comúnmente usado para accesar cuentas de otras personas.

**Sniffer:** Un sniffer es un programa que escucha todo el trafico de la red a la que esta conectada la computadora, aunque los datos no sean para él. Esto es posible por que la mayoria de las tarjetas de red ethernet tienen un modo llamado promiscuo, que les permite aceptar todos los datos de la red.

**Software:** Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquina.

**Spam:** Es el envío masivo de correos electrónicos a usuarios sin que estos lo hubieran solicitado. También se denominan así al envío intencionado de grandes cantidades de correo a un servidor en concreto con el objeto de colapsarlo.

**SSL:** *Secure Sockets Layer.* Es el protocolo diseñado por la empresa Netscape para proveer comunicaciones encriptadas en Internet. Los servicios de comercio electrónico que incluyen medios de pago usan este tipo de protocolos para establecer una conexión segura, encriptada, entre el servidor donde se realiza la compra y el ordenador desde donde se ejecuta la orden, con objeto de que la orden de compra que contenga los datos personales del comprador, especialmente el número de tarjeta de crédito, no pueda ser interceptada por otro usuario.

Este sistema de seguridad es imprescindible para realizar comercio electrónico, ya que al ser indispensable el uso de tarjeta de crédito para realizar todos los pagos, los consumidores necesitan garantías de que los procesos de pago son seguros.

**Tarifa Plana:** Se refiere a la modalidad de servicios que ofrecen operadoras o proveedores de servicio de Internet, mediante la cual los usuarios pueden navegar sin límite de tiempo por Internet por una cantidad fija mensual. La tarifa plana es un incentivo para el uso de Internet y favorece todas las actividades comerciales que se desarrollan en la red.

**Tempest.** (Transient Electromagnetic Pulse Surveillance Tecnology), son  especificaciones que los sistemas informáticos para el gobierno de EU deben cumplir.

**Terminal:** Puerta de acceso a una computadora. Puede tratarse de un monitor y teclado o de una computadora completa.

**Tráfico:** En relación con una red informática, se refiere al flujo y volumen de datos que circula por la misma. Si el trafico es muy alto los paquetes que circulan por la red pueden ralentizarse, y para evitar esto es necesario ampliarla con el objeto de que puedan circular más datos en el mismo tiempo. Para realizar procesos de comercio electrónico es necesario que se disponga de una red suficiente para absorber el tráfico que circula por la misma.

**Trashing:** Arte de revolver la basura para encontrar información útil.

**UNIX:** Sistema operativo utilizado por la gran mayoría de máquinas de Internet.

**Virus:** Es una serie de claves en código que adherirse a los programas legítimos y propagarse a otros programas informáticos. Hay varios tipos de virus, desde los que no hacen más que mostrar un mensaje, hasta los que destruyen todo lo que pueden del disco duro.

**Visualizador, Lector, Reader:** Son programas desarrollados por las compañías que han difundido sistemas para la creación de e-books. Estos programas permiten la visualización de los e-books al mismo tiempo que facilitan al usuario diversas opciones similares a las que podría realizar con un libro en papel, tales como subrayar, colocar notas, etc. Además incorporan diccionarios y otras utilidades electrónicas.

**ZAPPER:** Programa que se encarga de borrar los logs que graban las entradas, acciones y salidas de usuarios, por ejemplo cuando un hacker entra en un sistema debe ejecutar un zapper para no ser cazado.

**ANEXO II**

**Hacker manifiesto**

Uno más ha sido capturado hoy,

Está en todos los periódicos.

"Joven arrestado en Escándalo de Crimen por Computadora",

"Hacker arrestado luego de traspasar las barreras de seguridad de un banco. . ."

Malditos muchachos. Todos son iguales.

Pero tú, en tu psicología de tres partes y tu tecnocerebro de 1950, has alguna vez observado detrás de los ojos de un Hacker?

Alguna vez te has preguntado ¿qué lo mueve, qué fuerzas lo han formado, cuáles lo pudieron haber moldeado?

Soy un Hacker, entra a mi mundo. . .

El mío es un mundo que comienza en la escuela. . .

Soy más inteligente que la mayoría de los otros muchachos, esa basura que ellos nos enseñan me aburre. . .

Malditos subrealizados. Son todos iguales.

Estoy en la preparatoria.

He escuchado a los profesores explicar por decimoquinta vez como reducir una fracción.

Yo lo entiendo.

"No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente. . ."

Maldito muchacho. Probablemente se lo copió. Todos son iguales.

Hoy hice un descubrimiento.

Encontré una computadora.

Espera un momento, esto es lo máximo. Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué.

No porque no le gusto. . .

O se siente amenazada por mí. . .

O piensa que soy un engreído. . .

O no le gusta enseñar y no debería estar aquí. . .

Maldito muchacho. Todo lo que hace es jugar. Todos son iguales. Y entonces ocurrió. . . una puerta abierta al mundo. . .

Corriendo a través de las líneas telefónicas como la heroína a través de las venas de un adicto, se envía un pulso electrónico, un refugio para las incompetencias del día a día es buscado. . . una tabla de salvación es encontrada.

"Este es. . . este es el lugar a donde pertenezco. . ."

Los conozco a todos aquí. . .

Aunque nunca los hubiera conocido, o hablado con ellos, o nunca vuelva a escuchar de ellos otra vez. . .

Los conozco a todos. . .

Malditos muchachos. Enlazando las líneas telefónicas otra vez.

Todos son iguales. . .

Apuesta lo que sea a que todos somos iguales. . .

A nosotros nos han estado dando comida para bebés con cuchara en la escuela, cuando estábamos hambrientos de carne. . .

Las migajas de carne que ustedes dejaron escapar estaban masticadas y sin sabor.

Nosotros hemos sido dominados por sádicos, o ignorados por los apáticos.

Los pocos que tienen algo que enseñarnos encontraron alumnos complacientes, pero esos pocos son como gotas de agua en el desierto.

Ahora este es nuestro mundo. . .

El mundo del electrón y el conmutador, la belleza del Byte.

Nosotros hacemos uso de un servicio que ya existe sin pagar por lo que podría ser barato como el polvo, si no estuviera en manos de glotones hambrientos de ganancias,

Y ustedes nos llaman criminales.

Nosotros exploramos. . . y ustedes nos llaman criminales.

Nosotros buscamos detrás del conocimiento. . . y ustedes nos llaman criminales.

Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos. . . y ustedes nos llaman criminales.

Ustedes construyeron bombas atómicas,

Ustedes hicieron la guerra,

Ustedes asesinaron, engañaron y nos mintieron

Y trataron de hacernos creer que era por nuestro bien,

Ahora nosotros somos los criminales.

Si, soy un criminal.

Mi crimen es la curiosidad.

Mi crimen es el juzgar a las personas por lo que dicen y piensan, no por lo que aparentan.

Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás.

Soy un Hacker, este es mi manifiesto.

Tú podrás detener este esfuerzo individual, pero nunca podrás detenernos a todos. . . después de todo, todos somos iguales.

VIRUS:

Podemos utilizar una línea de tiempo para ver como fue creciendo este fenómeno:

1980

En los inicios de los años 80 comenzó la propagación de las computadoras personales apareciendo en los años 1981-1982 el virus Elkcloner destinado a infectarla.

1984

En mayo de ese año, aparece una variante simplificada del juego "Darwin" llamado "Core War" en el que los jugadores escriben programas en lenguaje ensamblador, los cuales, una vez que están siendo ejecutados en memoria luchan entre sí con el objetivo de bloquearse.

1985

A partir de 1985 se impuso en el mercado la computadora personal IBM con sistema operativo DOS la que, por el impetuoso desarrollo en su producción, provocó una reducción de los precios permitiendo así su amplia distribución en el mundo. De esta manera aumentó la cantidad de personas ocupadas activamente en su programación.

Esto, junto con el desarrollo de las redes de comunicación, permitió que la computadora no sólo fuera utilizada en los trabajos sino también en los hogares. Además, el hecho de ser el DOS un sistema operativo sumamente amigable, poco protegido, bastante documentado, al cual los fabricantes de dichas computadoras, incluyendo sus clones, contribuyendo a estandarizar, el proceso de inicialización de las mismas, tabla de vectores de interrupción, rutinas del BIOS y localizaciones de memoria provocó la creación de una enorme plataforma común para la propagación de los virus decomputadoras.

1986

Con la creación del virus Brain comenzó lo que se ha dado en llamar la segunda etapa en el desarrollo de los programas malignos. Este virus fue construido en Pakistán con el fin de castigar a los turistas norteamericanos que compraban en ese país copias ilegales de software barato.

1987

En noviembre de 1987 fue detectado en EEUU el virus LEHIGH que sólo infectaba al archivo COMMAND.COM y que una vez que realizaba 4 infecciones destruía la información contenida en los discos. Otros virus creados este año fueron:

Viena, Jerusalem, Stoned (primer virus que infectó al sector de particiones de los discos rígidos y el sector de arranque de los disquetes), Italian o Ping-Pong, Cascade (utilizaba una nueva idea y que era la de cifrar el código del virus con el fin de que varíe de un archivo infectado a otro) y el gusano CHRISTMAS.

1988

El año 1988 se destacó por la amplia propagación de los virus Stoned, Cascade, Jerusalem, Italian y Brain, lo que conllevó a la creación de los primeros antivirus.También se reportan en este año infecciones con virus tales como Dbase (que destruía la información de los archivos .DBF), Denzuk y Traceback, además éste fue el año cuando Morris propagó su programa (ya explicado anteriormente).

1989

En marzo de 1989 fue detectado el virus DATACRIME, elaborado en Holanda, el cual se propagó ampliamente; este virus, destruía la información de los discos rígidos formateando el cilindro 0 de los mismos.

Una de las hazañas más sorprendentes de intercambio de información entre hackers fue el caso Price. En esta ocasión, se investigó la acción de un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde allí conseguía entrar en los ordenadores del Ministerio de Defensa de los Estados Unidos. Llegó a copiar archivos que no eran materia reservada, pero sí investigaciones de temas delicados.

El centro de trabajo era su casa, en Londres, y desde allí causó uno de los mayores desastres informáticos de la década. No trabajaba solo, por lo que intercambió todos los documentos que había obtenido con hackers de distintos países, vía Internet. El caos fue total, llegando incluso al cierre temporal de la red norteamericana. Estos grupos tienen una forma de operar muy estricta, y la exclusión de uno de sus miembros significa la recesión total de privilegios, y la condena al ostracismo virtual. Fidelidad, confidencialidad y tenacidad son los rasgos más comunes entre los hackers.

(Pág Web Hackers.htm).

*NORMAS BASICAS DEL HACKER:*

1. Nunca dañes algo intencionadamente. Lo único que conseguirás será buscarte problemas.

2. Modifica solo lo estrictamente necesario para entrar y para evitar ser localizado, o para poder acceder otras veces.

3. No hackees nunca por venganza ni por intereses personales o económicos.

4. No hackees sistemas pobres que no puedan reponerse de un ataque fuerte. Ni tampoco sistemas muy ricos o grandes que puedan permitirse gastar dinero y tiempo en buscarte.

5. Odia a telefónica pero no te metas con ella.

6. No hackees ordenadores del gobierno. (El gran hermano te observa) Tal vez sean más emocionantes, pero no olvides que la policía trabaja para ellos.

7. No comentes con nadie, a menos que sea de total confianza, tus hazañas. (Los mas grandes hackers de la historia han sido cazados debido a las confesiones de sus novias)

8. Cuando hables en *BBS* o por Internet, procura ser lo mas discreto posible. Todo lo que digas quedará almacenado.

9. Se paranoico. Una da las características principales de los mejores hackers es la paranoia.

10. No dejes ningún dato que pueda relacionarse contigo, en los ordenadores que hackees. Y si es posible, ni siquiera "firmes".

11. Estudia mucho antes de lanzarte a la práctica.

12. Nunca dejes de estudiar y de aprender nuevas cosas, el mundo de la informática avanza rápidamente, y es necesario mantener un buen ritmo si no quieres quedarte atrás.

Algunos de estos consejos te parecerán anticuados y estúpidos, pero la mayoría tienen un doble objetivo. Mantener limpio el maltratado nombre de los hackers y evitarte problemas con la justicia.

Fuente: Documento recopilado ©eLectronic @ magaZine - 1997.

**BIBLIOGRAFÍA**

Almiron, Nuria (2002). *Los amos de la globalización*. España: Plaza & Janés Editores, S.A.

Baron, Robert A. (1996). *Psicología.* México: Editorial Prentice-Hall.

Buick, Joanna y Jevtiv, Zoran (1995). *Ciberespacio*. Buenos Aires: Era Naciente S.R.L.

Cabello, Vicente P. (2000). *Psiquiatría Forense en el derecho Penal*. Tomo 2. Buenos Aires: Editorial Hammurabi Srl.

Cebrián, Juan Luis (1998). *La Red*. Buenos Aires: Editorial Taurus.

*Código Penal y leyes complementarias* (1998). Buenos Aires: Editorial A-Z.

del Acebo Ibáñez, Enrique y Brie, Roberto J.(2001). *Diccionario de sociología.* Buenos Aires: Editorial Claridad.

Del Popolo, Juan H. (1996). *Psicología Jurídica*. Mendoza, Argentina: Editorial Jurídicas Cuyo.

Dormido, Sebastián y Mellado, Mariano (1984). *La Revolución Informática*. España: Editorial Salvat.

Freud, Sigmund (1923-25) Ordenamiento de James Strachey*. Volumen 19 El yo y el ello y otras obras. Los Vasallajes del Yo*: Standard Edition.

Garrido Genoves, Vicente y Redondo Illescas, Santiago (1997). *Manual de Criminología Aplicada.* Mendoza, Argentina: Editorial Jurídicas Cuyo.

Garrido, Vicente; Stangeland, Per y Redondo, Santiago (2001). *Principios de criminología*. España: Editorial Tirant Lo Blanch.

Garrone, José Alberto (1987). *Diccionario Manual Jurídico*. Buenos Aires: Editorial Abeledo-Perrot.

Gibson, William (1989). *Neuromante.* Barcelona, España: Editorial Minotauro.

Hernández Sampieri, Roberto; Fernández Collado, C. y Lucio, P. (2000). *Metodología de la investigación.* México: Editorial Mc Graw Hill. Segunda Edición.

Himanen, Pekka (2002). *La ética del hacker*. Buenos Aires: Editorial Destino.

Huerta, Marcelo y Líbano, Claudio (1996). *Delitos informáticos*. Chile: Editorial Jurídica ConoSur.

Kerlinger, Fred y Lee, Howard B. (2002). *Investigación del comportamiento*. México: Mc Graw-Hill.

Kreimer, Juan C y Tello, Nerio (2003). *Diccionario de Movimientos del Siglo XX*. Buenos Aires: Editorial Longseller.

La Prensa - Opinión – (10/04/2002) *Ciberpolicías y ciberdelitos*. Buenos Aires: Edición Nº 22694

León, Orfelio G. y Montero, Ignacio (1993). *Diseño de Investigaciones. Introducción a la lógica de la Investigación en Psicología y Educación.* Madrid, España: Mc Graw-Hill/Interamericana de España S.A.

Levy, Steven (1984). *Hackers*. España: Editorial Anchor/Doubleday.

Liberman, David y Maldavsky, David (1976). *Psicoanálisis y Semiótica*. Buenos Aires: Editorial Paidos.

Liberman, David (1978). *Comunicación y Psicoanálisis*. Buenos Aires: Alex Editor.

Marchiori, Hilda (1984). *Delito y personalidad*. Córdoba, Argentina: Lerner Editora.

Markoff, John y Hafner Katie (1991). *Cyberpunk*. EE.UU: Touchstone.

Palazzi, Pablo A. (2000). *Delitos Informáticos.* Buenos Aires: Editorial Ad Hoc S.R.L.

Pfaffenberger, Bryan (1999). *Diccionario de términos de computación e Internet.* México: Prentice Hall.

Radar suplemento literario de Página/12. (10/03/2002) Nota a Stallman: Copyright © 2001 Free Software Foundation, Inc.

Raymond, Eric (1991). *The New Hackers Dictionary*. EE.UU.: The MIT Press.

Sarra, Andrea Viviana (2000). *Comercio electrónico y derecho*. Buenos Aires: Editorial Astrea.

Scambray,Joel, Mc Clure, Stuart, Kurtz,George (2001). *Hackers 2.* España: Editorial Osborne Mc Graw-Hill.

Téllez Valdes, Julio (1996). *Derecho Informático*. México: Editorial Mc Graw Hill.

**CIBER-BIBLIOGRAFÍA**

**Páginas Web en Internet**

*Historias de hackers, crackers, phreakers y viruckers y estudios relacionados utilizados en esta tesis:*

www.aeapg.org.ar - Asociación Escuela Argentina de Psicoterapia para graduados Revista 12/13: David Liberman: La creatividad de un psicoanalista argentino

www.belt.es

www.bolivia.indymedia.org

www.ciencia.vanguardia.es

Comunidad hacker www. 2600.com

www.datosenlaweb.com

www.delitosinformaticos.com/trabajos/criminalista.pdf

www.delitosinformaticos:entendiendolosriesgosyelcuidadodelainformacion.htm

www.delitosionformaticos2.htm

www.fbi.gov

www.guardiacivil.org

How To Become A Hacker (http://www.tuxedo.org/~esr/faqs/hacker-howto.html )

www.interseguridad.com.ar/nota2.htm

www.jalisco.gob.mx/organismos/ijcf/orga.html

www.kevinmitnick.com

www.mailxmail/delitos.htm

www.mografias.com/delitos.htlm

www.olivet.com/astruc/doctxt06.htm

www.onething.com/archive/

www.panix.com/vtw/exon/exon.html

www.personal.redestb.es/hugo/byron/ini.htm

www.phantom.com/slowdog/

www.policia.gov.co/dijin/informaticos.htm

www.posta.arq.ucv.ve

www.Revista EXACTA mente - Divulgacion.htm

www.scjn.gob.mx

www.smoenelinteriordelamentedelconocedorinterno.htm

So you wanna be a hacker? ( http://www.accessorl.net )

www.ssp.gob.mx/\_k\_organos/pfp.html; Febrero 2003.

www.[terra.com.ar/](http://www.terra.com.ar/) tecnología

The complete Social Engineering FAQ! ( bernz@ix.netcom.com )

The Hacker Crackdown ( http://www.tuxedo.org/~esr/crackdown )

The Hacker FAQ ( http://www.plethora.net/~seebs/faqs/hacker.html )

The Jargon File ( http://www.tuxedo.org/~esr/jargon )

www.tiny.uasnet.mx/prof/cln/der/silvia/CPPPS.htm

www.tribunalmmm.gob.mx/Iej/inf\_jud/default.htm

www.tuxedo.org/jargon

www.ubik.to

www.ulpiano.com/recursos\_delitos.htm

www.umich.mx

www.usdoj.gov/criminal/cybercrime

www.vlex.com/mx

www.websitemaker.com/gorbato/magazine/nota4707.htm

*Estadísticas sobre delitos informáticos:*

www.aris.securityfocus.com

Computer Emergency Response Team (CERT); www.cert.org

www.isc.incidents.org

www.acert.gov.ar

www.aeapg.org.ar

www.rediris.es

*Derecho sobre delitos informáticos:*

www.criminologia.usal.es/guia/dp3.htm

www.csrc.ncsl.nist.gov/

www.derecho.org

www.derecho.unam.mx

es.wikipedia.org

www.estarinformado.com

www.juridicas.unam.mx

www.legislacionmundial.com

**María Marta Ruiz**

[martunet@hotmail.com](mailto:martunet@hotmail.com)

Tesis de Licenciatura en Psicología

Octubre de 2005.-

Categoría: Psicología. Jurídica. Perfiles de personalidad en el ciberespacio.

Universidad del Aconcagua. Mendoza. Argentina

1. Kreimer, Juan C, y Tello, Nerio. (2003) Diccionario de movimientos del siglo XX. Ed. Longseller. Buenos Aires. Pág. 91. [↑](#footnote-ref-1)
2. Kreimer – Tello. Op. cit. Pág. 92. [↑](#footnote-ref-2)
3. Ibídem. [↑](#footnote-ref-3)
4. Kreimer – Tello. Op. cit. Pág. 163. [↑](#footnote-ref-4)
5. Ibídem. [↑](#footnote-ref-5)
6. Ibídem. [↑](#footnote-ref-6)
7. Vélez Jahn, Gonzalo. Pág web posta.arq.ucv.ve [↑](#footnote-ref-7)
8. Sarra, Andrea. "Comercio electrónico y Derecho". Pág. 80. [↑](#footnote-ref-8)
9. Sarra, Andrea. Op cit. Pág. 80 [↑](#footnote-ref-9)
10. Ibídem. [↑](#footnote-ref-10)
11. Sarra, A. Op. cit. Pág. 31. [↑](#footnote-ref-11)
12. Buick, Joanna y Jevtic, Zoran. Ciberespacio para principiantes. Ed. Era Naciente. Bs. 1995. Pág. 4. [↑](#footnote-ref-12)
13. Gibson, William. Neuromancer. Pág. 72, 82 y 132. [Citado por Sarra, Op.cit. Pág. 81). [↑](#footnote-ref-13)
14. Sarra, A. Op. cit. Pág. 81. [↑](#footnote-ref-14)
15. Pfaffenberger, Bryan. Diccionario de términos de computación e Internet. Prentice Hall, México. 1999. Pág. 435. [↑](#footnote-ref-15)
16. Pagina web monografias.com [↑](#footnote-ref-16)
17. Sarra, Andrea. Op. cit. Pág 69. [↑](#footnote-ref-17)
18. Himanen, Pekka, “La ética del hacker". Pág 144-146 [↑](#footnote-ref-18)
19. Cebrián, Juan Luis. “La red”. Pág 18 [↑](#footnote-ref-19)
20. Pfaffenberger, Bryan. Op. cit. Pág. 263. [↑](#footnote-ref-20)
21. Pág. Web: tuxedo.org/jargon [↑](#footnote-ref-21)
22. Buick, Joanna y Jevtiv, Zoran “Ciberespacio”. Pág. 127 [↑](#footnote-ref-22)
23. Pág web ciencia.vanguardia.es/ciencia/portada/p351.html [↑](#footnote-ref-23)
24. Sarra, A. Op. cit. Pág. 85. [↑](#footnote-ref-24)
25. Ibídem. [↑](#footnote-ref-25)
26. Himanen, Pekka, Op. Cit.Pág 102-104 [↑](#footnote-ref-26)
27. Garrone, José Alberto “Diccionario Manual Jurídico” Ed. Abeledo-Perrot, Bs.As., 1987 [↑](#footnote-ref-27)
28. **Supremo Tribunal de Justicia del Estado de Sinaloa en pág web delitosinformaticos2.htm** [↑](#footnote-ref-28)
29. Lic. Manson, Marcelo en pág. web monografías.com [↑](#footnote-ref-29)
30. Sarzana, Carlo. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53. en pág. web delitosinformaticos2.htm [↑](#footnote-ref-30)
31. pag web delitos informaticos.htm [↑](#footnote-ref-31)
32. Téllez Valdes, Julio. Derecho Informático. 2da. edición. México. Ed. Mc Graw Hill 1996. Pp. 103-104. [↑](#footnote-ref-32)
33. Soto Campos, Joaquin en pág web mailxmail.com/delitosinformaticos.htm [↑](#footnote-ref-33)
34. Término que proviene del griego stratégema, que significa “engaño utilizando la astucia”. [↑](#footnote-ref-34)
35. Palazzi, Pablo “Delitos Informáticos”, Ad.Hoc, 2000, pág. 67. [↑](#footnote-ref-35)
36. Altmark, Daniel R.: Informática y Derecho, nº1, Depalma, Bs.As., 1987, p.17. En Palazzi. Op.cit. [↑](#footnote-ref-36)
37. Pag web usdoj.gov / criminal/ cybercrime [↑](#footnote-ref-37)
38. (20 vulnerabilidades más críticas de Internet, estudio realizado por Sans Institute y FBI, 2 de octubre de 2001 http://66.129.1.101/top20.htm). [↑](#footnote-ref-38)
39. Del Popolo, Juan H “Psicología Jurídica” Ed Jurídicas Cuyo, Mendoza, 1996. [↑](#footnote-ref-39)
40. Pág. web delitos informaticos: entendiendo los riesgos y el cuidado de la información.hmt [↑](#footnote-ref-40)
41. http://www.aeapg.org.ar Revista 12/13: David Liberman: La creatividad de un psicoanalista argentino [↑](#footnote-ref-41)
42. Obras Completas de Sigmund Freud, Standard Edition. Ordenamiento de James Strachey. Volumen 19 (1923-25) El yo y el ello y otras obras. Los Vasallajes del Yo. [↑](#footnote-ref-42)
43. Marchiori, Hilda. "Delito y personalidad". Ed. Lerner Editora Córdoba. 1984. Pág. 43. [↑](#footnote-ref-43)
44. Liberman, David. Comunicación y psicoanálisis. Alex Editor. Bs. Aires, 1978. Pág. 98 [↑](#footnote-ref-44)
45. Palazzi, Pablo “Delitos Informaticos”, Ad.Hoc, 2000, pág. 67. [↑](#footnote-ref-45)
46. Pág Web estarinformado.com. [↑](#footnote-ref-46)
47. Pág Web Smoenelinteriordelamentedelconocedorinterno.htm [↑](#footnote-ref-47)
48. Baron Robert A. “Psicología”, Ed. Prentice-Hall, México, 1996. [↑](#footnote-ref-48)
49. Ver glosario [↑](#footnote-ref-49)
50. Idem [↑](#footnote-ref-50)
51. del Acebo Ibáñez, Enrique y Brie, Roberto J. Diccionario de sociología. Ed. Claridad. Buenos Aires, 2001. Pág. 223-226. [↑](#footnote-ref-51)